**DEPARTMENT OF THE NAVY**
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

IN REPLY REFER TO

**SECNAVINST 5510.36 CH-2**
**N09N2**
**23 January 2001**

SECNAV INSTRUCTION 5510.36 CHANGE TRANSMITTAL 2

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION SECURITY PROGRAM (ISP) REGULATION

Encl: (1) Revised page 10-6 of Chapter 10

1. Purpose: To transmit a change to the DON ISP concerning the requirements for the residential storage of Secret and Confidential information.

2. Action: Remove page 10-6 of the basic instruction and replace with enclosure (1).

Richard Danzig

Distribution:
SNDL Parts 1 and 2
MARCORPS Code PCN 710000000000 and 71000000100

**DEPARTMENT OF THE NAVY**
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

IN REPLY REFER TO

**SECNAVINST 5510.36 CH-1**
**N09N2**
**19 June 2000**

SECNAV INSTRUCTION 5510.36 CHANGE TRANSMITTAL 1

From: Secretary of the Navy
To: All Ships and Stations

Subj : DEPARTMENT OF THE NAVY (DON) INFORMATION SECURITY PROGRAM (ISP) REGULATION

Encl: (1) Revised page 4

1. Purpose: To transmit an addition to the policies and procedures governing the DON ISP.

2. Action: Remove page 4 and replace with enclosure (1) of this change transmittal.

Richard Danzig

DISTRIBUTION:
SNDL Parts 1 and 2
MARCORPS Code PCN 21600401000

DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20350

SECNAVINST 5510.36
09N
17 March 1999

SECNAV INSTRUCTION 5510.36

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION SECURITY PROGRAM (ISP) REGULATION

Encl: (1) Subject regulation

1. Purpose

a. To establish uniform ISP policies and procedures.

b. To implement Executive Order (E.O.) 12958, "Classified National Security Information," which directs agencies to observe the democratic principles of openness and the free flow of information, as well as to enforce protective measures for safeguarding information critical to the national security.

c. To incorporate policies and procedures established by other executive branch agencies.

2. Cancellation. SECNAVINST 5510.30A, "Department of the Navy (DON) "Personnel Security Program Regulation," (PSP) cancels chapters 20 through 24 of OPNAVINST 5510.1H of 29 April 1988, "Department of the Navy Information and Personnel Security Program Regulation." Report Symbols OPNAV 5510-6F and 5510-6Q are also cancelled. Enclosure (1) (hereafter referred to as "this regulation") cancels the remainder of OPNAVINST 5510.1H which addressed the ISP and the National Industrial Security Program (NISP).

3. Objective. To achieve uniform implementation of ISP policy and procedures throughout the DON by pro-active command programs that accomplish the purpose of enclosure (1). Further, this regulation and SECNAVINST 5510.30A complement each other and have been coordinated to achieve compatibility.

4. Scope. This regulation encompasses all classified national security information (NSI) classified under E.O. 12958, and predecessor orders, and special types of classified and controlled unclassified information outlined in chapter 1. It applies to all commands and to all military and civilian personnel of the DON.

5. Summary of Changes. Major changes to this regulation were mandated by E.O. 12958 concerning classified NSI and E.O. 12829 concerning the NISP; a revised Director of Central Intelligence Directive (DCID) on security controls for the dissemination of intelligence information; a Department of Energy (DOE) regulation on nuclear classification and declassification; and a reissued Department of Defense (DoD) 5200.1-R on the ISP. Changes in this regulation include:

a. **General**. Issues this regulation as a Secretary of the Navy instruction to include the United States Marine Corps; updates and verifies all citations and references; consolidates related subjects; and reorganizes policies and procedures into chapters reflecting a life-cycle concept of classified information, from creation to disposition.

b. **Chapter 1. Introduction to the ISP**. Defines the "Purpose" to encompass the implementation of all laws, E.O.s, federal regulations, DCIDs and DoD guidance on the ISP and related programs; provides guidance on the NISP; includes references to controlled unclassified information; prescribes basic policy guidance; addresses combat operations; discusses waivers and exceptions, and alternative or compensatory measures; and outlines the new national, DoD and DON organizations for security matters.

c. **Chapter 2. Command Security Management**. Redefines responsibilities and duties of the commanding officer, security manager and other security positions; emphasizes the requirement for supervisors to evaluate command personnel performing security duties; emphasizes the importance of classification challenges when appropriate; provides emergency planning guidance; deletes security points of contact; and updates forms, reports and the security inspection checklist.

d. **Chapter 3. Security Education**. States the security education requirements unique to the ISP; cites the SECNAVINST 5510.30A as the regulation covering all other security education requirements.

e. **Chapter 4. Classification Management**. Combines previous chapters on classification, upgrading, declassification and downgrading; states E.O. 12958 classification criteria, discusses classification challenges, rules for duration of classification, provisions for automatic declassification; requires training of Original Classification Authorities (OCAs); and updates the OCA listing.

f. **Chapter 5. Security Classification Guides (SCGs).** Updates the list of Retrieval and Analysis of Navy Classified Information (RANKIN) Program guides; and provides guidance on resolving conflicts between source documents and SCGs.

g. **Chapter 6. Marking.** Consolidates and expands marking guidance, to include intelligence information and Naval Nuclear Propulsion Information (NNPI); prescribes new marking requirements, including the marking requirements for controlled unclassified information; and provides an expanded marking exhibit.

h. **Chapter 7. Safeguarding.** Consolidates all safeguarding requirements for classified NSI; the policy concerning the reproduction of classified information; adds control measures governing special types of classified and controlled unclassified information; updates working paper guidance; eliminates two-person integrity and the entry/exit program; and adds policy for alternative or compensatory control measures.

i. **Chapter 8. Dissemination.** Consolidates guidance on dissemination, to include distribution statements for technical documents and prepublication review of information proposed for public release.

j. **Chapter 9. Transmission or Transportation.** Consolidates and condenses previous guidance; updates policy on the use of the General Services Administration (GSA) contract carrier; clarifies use of the form DD 2501; and adds an exhibit concerning transmission to foreign governments.

k. **Chapter 10. Storage and Destruction.** Updates storage and secure room construction standards and policy governing frequency of combination changes; and eliminates the required use of form OPNAV 5511/12, "Classified Material Destruction Report," to record the destruction of classified information.

l. **Chapter 11. Industrial Security Program.** Consolidates and updates all policies and procedures for implementation of the NISP.

m. **Chapter 12. Loss or Compromise of Classified Information.** Prescribes actions to take in the event of a security discrepancy, loss or compromise of classified information; and provides expanded exhibits concerning

Preliminary Inquiry and Judge Advocate General Manual (JAGMAN) Investigation narrative formats.

6. **Action.** Each DON commanding officer shall establish and conduct an ISP in compliance with this regulation.

7. **Violations of this Regulation**

a. **Military Personnel.** Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this regulation.

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

8. **Records Disposition.** Disposition requirements for records related to the ISP are based upon schedules approved by the Archivist of the United States and listed in SECNAVINST 5212.5D, Navy and Marine Corps Records Disposition Manual.

9. **Reports and Forms**

a. **Reports.** The reporting requirements imposed by this regulation have been approved by the Navy Records Manager and are assigned the report control symbols identified in appendix C.

b. **Forms.** Information regarding procurement of forms used in the ISP appears in appendix B.

Richard Danzig

Distribution:
SNDL Parts 1 and 2
MARCORPS Codes PCN 21600401000

# TABLE OF CONTENTS

PARAGRAPH PAGE

**Chapter 1: Introduction to the Information Security Program**

1-1 Purpose, Applicability, and Scope . . . . . 1-1
1-2 Policy Guidance . . . . . 1-3
1-3 National Authorities for Security Matters . . . . . 1-4
1-4 DoD Security Program Management . . . . . 1-5
1-5 DON Security Program Management . . . . . 1-6

**Chapter 2: Command Security Management**

2-1 Commanding Officer . . . . . 2-1
2-2 Security Manager . . . . . 2-2
2-3 Top Secret Control Officer (TSCO) . . . . . 2-4
2-4 Other Security Assistants . . . . . 2-4
2-5 Security Related Collateral Duties . . . . . 2-5
2-6 Contracting Officer's Representative (COR) . . . . . 2-6
2-7 Information Systems Security Manager (ISSM) . . . . . 2-6
2-8 Special Security Officer (SSO) . . . . . 2-6
2-9 Security Officer . . . . . 2-7
2-10 Security Servicing Agreements (SSAs) . . . . . 2-7
2-11 Inspections, Assist Visits, and Program Reviews . . . 2-8
2-12 Forms . . . . . 2-8
2-13 Report Control Symbols . . . . . 2-8
Exhibit 2A - Guidelines for Command Security Instruction . . . . . 2A-1
Exhibit 2B - Emergency Plan and Emergency Destruction Supplement . . . . . 2B-1
Exhibit 2C - Security Inspection Checklist . . . . . 2C-1

**Chapter 3: Security Education**

3-1 Basic Policy . . . . . 3-1
3-2 Responsibility . . . . . 3-1
3-3 Additional Information Security Education . . . . . 3-1

**Chapter 4: Classification Management**

4-1 Basic Policy . . . . . 4-1
4-2 Classification Levels . . . . . 4-1
4-3 Original Classification . . . . . 4-2
4-4 Original Classification Authority . . . . . 4-2
4-5 Requests for Original Classification Authority . . . . 4-2
4-6 OCA Training . . . . . 4-3

4-7 Original Classification Criteria, Principles, and Considerations . . . . . 4-3
4-8 Duration of Original Classification . . . . . 4-3
4-9 Derivative Classification . . . . . 4-5
4-10 Accountability of Classifiers . . . . . 4-5
4-11 Limitations on Classifying . . . . . 4-5
4-12 Classification Challenges . . . . . 4-6
4-13 Resolution of Conflicts Between OCAs . . . . . 4-7
4-14 Tentative Classification . . . . . 4-7
4-15 Patent Secrecy Information . . . . . 4-8
4-16 Independent Research and Development Information (IR&D)/Bid and Proposal (B&P) . . . . . 4-8
4-17 Foreign Government Information (FGI) . . . . . 4-9
4-18 Naval Nuclear Propulsion Information (NNPI) . . . . . 4-10
4-19 Authority to Downgrade, Declassify or Modify Classified Information . . . . . 4-10
4-20 Declassification by the Director of the ISOO . . . . . 4-11
4-21 Automatic Declassification . . . . . 4-11
4-22 Systematic Declassification Review . . . . . 4-11
4-23 Mandatory Declassification Review . . . . . 4-12
4-24 Information Exempted from Mandatory Declassification Review . . . . . 4-13
4-25 Classified Information Transferred to the DON . . . . 4-13
4-26 Notification of Classification Changes . . . . . 4-14
4-27 Foreign Relations Series . . . . . 4-15
Exhibit 4A - DON Original Classification Authorities . . . . . 4A-1

**Chapter 5: Security Classification Guides**

5-1 Basic Policy . . . . . 5-1
5-2 Preparing SCGs . . . . . 5-1
5-3 RANKIN Program . . . . . 5-1
5-4 Periodic Review of SCGs . . . . . 5-3
5-5 SCGs of Multi-Service Interest . . . . . 5-3
5-6 Conflict Between a Source Document and an SCG . . . . 5-3

**Chapter 6: Marking**

6-1 Basic Policy . . . . . 6-1
6-2 DON Command and Date of Origin . . . . . 6-2
6-3 Overall Classification Level Marking . . . . . 6-2
6-4 Interior Page Markings . . . . . 6-2
6-5 Portion Markings . . . . . 6-3
6-6 Subjects and Titles . . . . . 6-4
6-7 Placement of Associated Markings . . . . . 6-4
6-8 Marking Originally Classified Documents with the "Classified By" and "Reason" Lines . . . . . 6-5

6-9 Marking Derivatively Classified Documents with the "Derived From" Line . . . . . 6-5
6-10 Use of the "Downgrade To" and "Declassify On" lines. . 6-6
6-11 Warning Notices . . . . . 6-6
6-12 Intelligence Control Markings . . . . . 6-11
6-13 Marking Documents Classified Under the Patent Secrecy Act . . . . . 6-13
6-14 Independent Research and Development (IR&D) . . . . . 6-14
6-15 Marking Documents Containing NATO or FGI . . . . . 6-15
6-16 Translation. . . . . 6-16
6-17 Nicknames, Exercise Terms and Code Words . . . . . 6-16
6-18 Classification by Compilation. . . . . 6-17
6-19 Changes to Existing Classified Document. . . . . 6-17
6-20 Marking Training or Test Documents . . . . . 6-18
6-21 Marking Classified Documents with Component Parts. . . 6-18
6-22 Remarking Upgraded, Downgraded or Declassified Documents. . . . . 6-18
6-23 Classifying From Source Documents with Old Declassification Instructions . . . . . 6-19
6-24 Correspondence and Letters of Transmittal . . . . . 6-19
6-25 Marking Electronically-Transmitted Classified Messages . . . . . 6-21
6-26 Marking Classified Files, Folders and Groups of Documents . . . . . 6-22
6-27 Marking Classified Blueprints, Schematics, Maps and Charts . . . . . 6-22
6-28 Marking Classified Photographs, Negatives, and Unprocessed Film . . . . . 6-22
6-29 Marking Classified Slides and Transparencies . . . . . 6-23
6-30 Marking Classified Motion Picture Films and Videotapes . . . . . 6-23
6-31 Marking Classified Sound Recordings . . . . . 6-23
6-32 Marking Classified Microforms . . . . . 6-23
6-33 Marking Classified Removable AIS Storage Media . . . . 6-24
6-34 Marking Classified Documents Produced by AIS Equipment . . . . . 6-24
6-35 Marking Miscellaneous Classified Material . . . . . 6-25
Exhibit 6A - Sample Classified Document Markings . . . 6A-1
Exhibit 6B - Sample Marking of Classified U.S. Message Text Format (USMTF) Messages. . . 6B-1
Exhibit 6C - Equivalent Foreign Security Classifications . . . . . 6C-1

**Chapter 7: Safeguarding**

7-1 Basic Policy . . . . . 7-1
7-2 Applicability of Control Measures . . . . . 7-1
7-3 Top Secret Control Measures. . . . . 7-1

7-4 Secret Control Measure . . . . . 7-2
7-5 Confidential Control Measures . . . . . 7-2
7-6 Working Papers . . . . . 7-3
7-7 Special Types of Classified and Controlled Unclassified Information . . . . . 7-3
7-8 Alternative or Compensatory Control Measures . . . . . 7-5
7-9 Care During Working Hours . . . . . 7-6
7-10 End-of-Day Security Checks . . . . . 7-7
7-11 Safeguarding During Visits . . . . . 7-7
7-12 Safeguarding During Classified Meetings . . . . . 7-7
7-13 Reproduction . . . . . 7-10

**Chapter 8: Dissemination**

8-1 Basic Policy . . . . . 8-1
8-2 Top Secret . . . . . 8-1
8-3 Secret and Confidential . . . . . 8-1
8-4 Special Types of Classified and Controlled Unclassified Information . . . . . 8-1
8-5 Dissemination of Intelligence Information . . . . . 8-3
8-6 Dissemination to Congress . . . . . 8-3
8-7 Dissemination of Technical Documents . . . . . 8-3
8-8 Prepublication Review . . . . . 8-4
Exhibit 8A - Procedures for Assigning Distribution Statements on Technical Documents . . . . 8A-1
Exhibit 8B - Categories of Information which Require Review and Clearance by the ASD(PA) Prior to Public Release . . . . . 8B-1

**Chapter 9: Transmission and Transportation**

9-1 Basic Policy . . . . . 9-1
9-2 Top Secret . . . . . 9-1
9-3 Secret . . . . . 9-2
9-4 Confidential . . . . . 9-4
9-5 Special Types of Classified and Controlled Unclassified Information . . . . . 9-4
9-6 Telephone Transmission . . . . . 9-6
9-7 Classified Bulky Freight Shipments . . . . . 9-6
9-8 Preparing Classified Information for Shipment. . . . . 9-6
9-9 Addressing Classified Information for Shipment . . . . 9-7
9-10 Receipting for Classified Information . . . . . 9-8
9-11 General Provisions for Escorting or Handcarrying Classified Information . . . . . 9-9
9-12 Authorization to Escort or Handcarry Classified Information . . . . . 9-11

9-13 Authorization Letter for Escorting or Handcarrying Classified Information Aboard Commercial Passenger Aircraft . . . . . 9-12
9-14 Escort or Handcarry of Classified Information to the U.S. Senate . . . . . 9-13
Exhibit 9A - Transmission or Transportation to Foreign Governments . . . . . 9A-1
Exhibit 9B - Record of Receipt (OPNAV 5511/10) . . . . 9B-1

**Chapter 10: Storage and Destruction**

10-1 Basic Policy . . . . . 10-1
10-2 Standards for Storage Equipment . . . . . 10-1
10-3 Storage Requirements . . . . . 10-1
10-4 Procurement of New Storage Equipment . . . . . 10-4
10-5 Removal of Security Containers . . . . . 10-4
10-6 Shipboard Containers and Filing Cabinets . . . . . 10-4
10-7 Vaults and Secure Rooms. . . . . 10-5
10-8 Specialized Security Containers . . . . . 10-5
10-9 Non GSA-Approved Security Containers . . . . . 10-6
10-10 Residential Storage. . . . . 10-6
10-11 Replacement of Combination Locks . . . . . 10-6
10-12 Combinations . . . . . 10-7
10-13 Key and Padlock Control. . . . . 10-8
10-14 Securing Security Containers . . . . . 10-8
10-15 Repair, Maintenance, and Operating Inspections . . . . 10-8
10-16 Electronic Security System (ESS) . . . . . 10-10
10-17 Destruction of Classified Information . . . . . 10-11
10-18 Destruction Methods and Standards . . . . . 10-11
10-19 Destruction Procedures . . . . . 10-12
10-20 Destruction of Controlled Unclassified Information . . 10-12
10-21 Disposition of Classified Information From Commands Removed from Active Status or Turned Over to Friendly Foreign Governments . . . . . 10-13
Exhibit 10A - Vault and Secure Room (Open Storage Area) Construction Standards . . . . . 10A-1
Exhibit 10B - Priority for Replacement . . . . . 10B-1
Exhibit 10C - Maintenance Record for Security Containers/Vault Doors Optional Form 89 . . . . . 10C-1
Exhibit 10D - IDS and Access Controls . . . . . 10D-1

**Chapter 11: Industrial Security Program**

11-1 Basic Policy . . . . . 11-1
11-2 Authority . . . . . 11-1
11-3 Defense Security Service (DSS) Industrial Security Mission . . . . . 11-2

11-4 Clearance Under the NISP . . . . . 11-2
11-5 DSS and Command Security Oversight of Cleared DoD Contractor Operations . . . . . 11-2
11-6 Facility Access Determination (FAD) Program . . . . . 11-4
11-7 Contract Security Classification Specification (DD 254) . . . . . 11-4
11-8 COR Industrial Security Responsibilities . . . . . 11-4
11-9 Contractor Badges . . . . . 11-6
11-10 Visits by Cleared DoD Contractor Employees . . . . . 11-6
11-11 Contractor Facility Clearances . . . . . 11-6
11-12 Transmission or Transportation . . . . . 11-7
11-13 Disclosure . . . . . 11-7
11-14 Release of Intelligence to Cleared DoD Contractors . . 11-9
11-15 Prohibited Release of Intelligence . . . . . 11-10
11-16 Sanitization of Intelligence . . . . . 11-11
Exhibit 11A - Contract Security Classification Specification (DD 254) . . . . . 11A-1

**Chapter 12: Loss or Compromise of Classified Information**

12-1 Basic Policy . . . . . 12-1
12-2 Reporting Responsibilities . . . . . 12-1
12-3 Preliminary Inquiry (PI) . . . . . 12-2
12-4 Preliminary Inquiry Initiation . . . . . 12-2
12-5 Contents of the PI Message or Letter . . . . . 12-2
12-6 Classification of the PI Message or Letter . . . . . 12-2
12-7 Actions Taken Upon PI Conclusion . . . . . 12-3
12-8 Reporting Losses or Compromises of Special Types of Classified Information and Equipment . . . . . 12-3
12-9 JAGMAN Investigations . . . . . 12-5
12-10 JAGMAN Initiation and Appointment Letter . . . . . 12-5
12-11 Investigative Assistance . . . . . 12-6
12-12 Classification of JAGMAN Investigations . . . . . 12-6
12-13 Results of JAGMAN Investigations . . . . . 12-6
12-14 Review and Endorsement of JAGMAN Investigations by Superiors . . . . . 12-6
12-15 Security Reviews . . . . . 12-7
12-16 Classification Reviews . . . . . 12-7
12-17 Damage Assessments . . . . . 12-8
12-18 Public Media Compromises . . . . . 12-9
12-19 Security Discrepancies Involving Improper Transmissions . . . . . 12-10
Exhibit 12A - Sample PI Letter Format . . . . . 12A-1
Exhibit 12B - Sample PI Message Format . . . . . 12B-1
Exhibit 12C - Sample JAGMAN Appointment Letter . . . . 12C-1
Exhibit 12D - Sample JAGMAN Investigation Format . . . 12D-1
Exhibit 12E - Security Discrepancy Notice (OPNAV 5511/51) . . . . . 12E-1

**APPENDICES**

A Definitions and Abbreviations . . . . . A-1
B Forms . . . . . B-1
C Report Control Symbols . . . . . C-1

# CHAPTER 1

# INTRODUCTION TO THE INFORMATION SECURITY PROGRAM

## 1-1 PURPOSE, APPLICABILITY, AND SCOPE

1. **Purpose**

a. This regulation establishes the Department of the Navy (DON) Information Security Program (ISP). The ISP applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission and destruction of classified information. This regulation also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this regulation to include classified material (i.e., any matter, document, product, or substance on or in which classified information is recorded or embodied).

b. It implements the ISP within the DON in compliance with references (a) through (e), and also implements specific requirements of references (f) through (h).

2. **Applicability.** This regulation applies to all personnel, military and civilian, assigned to or employed by any element of the DON. Personnel are individually responsible for compliance. This regulation establishes the minimum standards for classification, safeguarding, transmission and destruction of classified information as required by higher authority.

3. **Scope.** This regulation applies to all official information that has been determined under reference (a) or any predecessor Order to require protection against unauthorized disclosure and is so designated by an appropriate classifying authority. This regulation incorporates the policies of documents referenced in paragraph 1-1.1b and refers to other directives listed at the end of each chapter that relate to the protection of classified information. Each chapter also lists related documents governing other classified programs, controlled unclassified information, and the National Industrial Security Program (NISP).

4. **Special Types of Classified Information.** Certain information is governed by other regulations (see **appendix A** for definitions):

a. **Communications Security (COMSEC) Information.** COMSEC information is governed by references (i) and (ab).

b. **Sensitive Compartmented Information (SCI).** SCI is governed by reference (j) and other national, Department of Defense (DoD), and DON issuances.

c. **Special Access Programs (SAPs).** All SAPs must be authorized by the Secretary of Defense (SECDEF) or the Deputy SECDEF and are governed by references (l) through (o). The Director, Special Programs Division (N89) receives and reviews requests for SAPs and the Under Secretary of the Navy must formally approve the establishment of each SAP in coordination with the Deputy SECDEF.

d. **Single Integrated Operational Plan (SIOP) and Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).** SIOP and SIOP-ESI is governed by reference (p), which is issued by the CNO (N514).

e. **Naval Nuclear Propulsion Information (NNPI).** NNPI is governed by reference (q). Certain NNPI may be unclassified but is marked with special handling instructions per reference (q).

f. **Restricted Data (RD) and Formerly Restricted Data (FRD).** RD and FRD is governed by reference (r) and the Department of Energy (DOE) Regulations issued by reference (h). **Critical Nuclear Weapons Design Information (CNWDI)** is a special category of RD whose access is governed by reference (s).

g. **Foreign Government Information (FGI).** FGI is information received from one or more foreign governments or international organizations as classified, or expected to be held in confidence. It is classified, safeguarded, and declassified as agreed between the United States (U.S.) and the foreign entity.

h. **North Atlantic Treaty Organization (NATO) Information.** NATO classified and unclassified information is governed by reference (t), which is issued by reference (u).

5. **NISP.** The NISP was established by reference (f) to safeguard classified information released to industry in a manner that is equivalent to its protection within the executive branch. It is the single, integrated, cohesive industrial security program of the U.S. to protect classified information in the possession of the contractors of all executive branch departments and agencies. The NISP applies to information classified under references (a) and (r).

6. **Controlled Unclassified Information.** Controlled unclassified information is defined and governed by laws, international agreements, E.O.s, and regulations that address the identification, marking, protection, handling, transmission, transportation, and destruction of controlled unclassified information. This regulation refers to the appropriate governing authority for these categories of controlled unclassified information:

a. For Official Use Only (FOUO) information under the Freedom of Information Act (FOIA);

b. Department of State (DOS) Sensitive But Unclassified (SBU) (formerly Limited Official Use (LOU)) information;

c. DoD and DOE Unclassified Controlled Nuclear Information (UCNI);

d. Drug Enforcement Administration (DEA) Sensitive Information;

e. Sensitive Information as defined by the Computer Security Act of 1987;

f. Unclassified information in technical documents requiring distribution statements and unclassified NNPI.

**1-2 POLICY GUIDANCE**

1. **Assistance Via the Chain of Command.** DON personnel are encouraged to obtain guidance or interpretation of policy and procedures in this regulation via the chain of command. Telephone inquiries may be made to the CNO (N09N2) **Security Action Hotline** at (202) 433-8856. See the CNO (N09N2) Homepage at **www.navysecurity.navy.mil**. After hours calls are recorded and returned as soon as possible.

2. **Combat Operations.** Commanding officers may modify the safeguarding requirements of this regulation as necessary to meet local conditions during combat or combat-related operations. Even under these circumstances, the provisions of this regulation shall be followed as closely as possible. This exception does not apply to regularly scheduled training exercises or operations.

3. **Waivers and Exceptions.** When conditions exist that prevent compliance with a specific safeguarding standard or costs of

compliance exceed available resources, a command may submit a request for a waiver or exception to the requirements of this regulation, in writing, via the chain of command to the CNO (N09N2). Each request shall include a complete description of the problem and describe the compensatory procedures, as appropriate. The initiating command shall assign a number using the command's Unit Identification Code (UIC) preceded by N for Navy or M for Marine Corps, W(I) for waiver or E(I) for exception, number, and year (e.g., N12345-E(I)-01-98) to each waiver or exception request. Include a point of contact and telephone number with your request. Waivers and exceptions are self-cancelling at the end of the approved time, unless a renewal request is approved by the CNO (N09N2).

a. **Waiver.** A waiver may be granted to provide temporary relief from a specific requirement pending completion of action which will result in compliance with this regulation.

b. **Exception.** An exception may be granted to accommodate a long-term or permanent inability to meet a specific requirement.

4. **Alternative or Compensatory Security Control Measures.** References (c) and (e) authorize the DON to employ alternative or compensatory security controls for safeguarding classified information. Procedures for submitting requests and requirements for approval are stated in chapter 7, paragraph 7-8.

## 1-3 NATIONAL AUTHORITIES FOR SECURITY MATTERS

1. **The President** of the U.S. bears executive responsibility for the security of the Nation which includes the authority to classify information for the protection of the national defense and foreign relations of the U.S. The President established standards for the classification, safeguarding, downgrading, and declassification of classified national security information (NSI) in reference (a).

2. **The National Security Council (NSC)** provides overall policy guidance on information and personnel security.

3. **The Director of the Information Security Oversight Office (ISOO)**, under the authority of the Archivist of the U.S., acting in consultation with the NSC, issues directives as necessary to implement reference (a). The directives establish national

standards for the classification and marking of classified national security information, security education and training programs, self-inspection programs, and declassification. The ISOO has the responsibility to oversee agency implementation and compliance with these directives. In this role, the ISOO conducts oversight visits at selected locations. Visits to or requests for information regarding DON commands are coordinated through the CNO (N09N2).

4. **The Security Policy Board (SPB)** is an interagency organization co-chaired by the Deputy SECDEF and the Director of Central Intelligence (DCI) created by the President to consider, coordinate, and recommend for implementation to the President, through the NSC, uniform standards, policies and procedures governing classified information and personnel security, to be implemented and applicable throughout the Federal Government.

5. **The DCI**, as the chairman of the National Foreign Intelligence Board (NFIB), issues instructions in the form of DCI directives or policy statements affecting intelligence policies and activities. The DCI is charged by reference (v) with protecting intelligence sources and methods.

6. **The Federal Bureau of Investigation (FBI)** is the primary internal security agency of the U.S. Government. It has jurisdiction over investigative matters which include espionage, sabotage, treason, and other subversive activities. The Director, Naval Criminal Investigative Service (DIRNCIS) is the investigative component of the DON and is the sole liaison with the FBI on internal security matters.

## 1-4 DoD SECURITY PROGRAM MANAGEMENT

1. **The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (OASD($C^3I$))** is the DoD senior official charged by the SECDEF with responsibility for developing policies and procedures governing information and personnel security, including atomic energy policy programs. The Deputy Assistant Secretary of Defense (Security and Information Operations (S&IO)) produces references (e) and (w). Reference (e) is the primary source for the policies and procedures in this regulation.

2. **The Under Secretary of Defense for Policy (USD(P))** is designated as the senior official responsible for administering that portion of the DoD ISP pertaining to SAPs, the National Disclosure Policy (NDP), FGI (including NATO), and security arrangements for international programs.

3. **The Deputy Under Secretary of Defense for Policy Support (DUSD(PS))** administers international security policy and performs administrative support to the SECDEF who is designated the U.S. Security Authority for NATO (USSAN). The USSAN implements security directives issued by NATO and oversees the Central U.S. Registry (CUSR), with Army as executive agency.

4. **The National Security Agency (NSA)** provides centralized coordination and direction for signals intelligence and communications security for the U.S. Government. The DON contributes to these efforts primarily through the Commander, Naval Security Group Command (COMNAVSECGRU). The Director, NSA is authorized by the SECDEF to prescribe procedures or requirements, in addition to those in DoD regulations, for SCI and COMSEC. The authority to lower any COMSEC security standards within the DoD rests with the SECDEF.

5. **The Defense Intelligence Agency (DIA)** coordinates the intelligence efforts of the Departments of the Army, Navy, and Air Force and is responsible for development of standards, implementation, and operational management of the SCI compartments for the DoD. The Director is the Senior Official of the Intelligence Community (SOIC) of the DoD and is a member of the NFIB.

## 1-5 DON SECURITY PROGRAM MANAGEMENT

1. **The Secretary of the Navy (SECNAV).** The SECNAV is responsible for implementing an ISP per the provisions of E.O.s, public laws, and directives issued by the NSC, DOE, DoD, DCI, and other agencies regarding the protection of classified information.

2. **The Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N)/DIRNCIS).** The SECNAV has designated the CNO (N09N)/DIRNCIS as the DON senior agency official under reference (a) and the DON RD management official under reference (h). The Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant

Director, Information and Personnel Security Programs (NCIS-21) provides staff support for these functions and responsibilities.

a. The CNO (N09N) is responsible to the SECNAV for establishing, directing, and overseeing an effective DON ISP, and for implementing and complying with all directives issued by higher authority. This responsibility includes:

(1) Formulating policies and procedures, issuing directives, and monitoring, inspecting, and reporting on the status of administration of the ISP in the DON.

(2) Implementing an industrial security program within the DON.

(3) Ensuring that persons with access to RD (including CNWDI) and FRD information are trained on appropriate classification, handling, and declassification procedures; serving as the primary point of contact for coordination with the DOE Director of Declassification on RD and FRD classification and declassification issues.

(4) Serving as primary ISP liaison with the ISOO, SPB, Office of the SECDEF and other DoD components and Federal agencies.

b. The CNO (N09N) is also responsible for establishing, administering, and overseeing the DON Personnel Security Program (PSP), and issues personnel security policy and procedures in reference (x), and publishes the Information and Personnel Security Newsletter on a quarterly basis. This newsletter is not a directive, but states the DON interpretation of security policies and procedures and provides advance notification of changes in the program. A roster of personnel assigned to the CNO (N09N2), showing each area of responsibility, is published periodically. Telephonic requests for information may be directed to the specialist having responsibility for the area of concern.

c. The DIRNCIS is responsible for investigative, law enforcement, physical security technical surveillance countermeasures, and counterintelligence (CI) policy and programs within the DON. DIRNCIS serves as the Assistant for Counterintelligence (N2E) to the Director of Naval Intelligence (DNI), and NCIS supports the national CI effort by collecting, analyzing, and disseminating information of internal security significance to DON commands.

3. **The Department of the Navy, Chief Information Officer (CIO), Office of the Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN(RD&A))** is responsible for DON implementation of reference (y). The DON CIO issues DON policies and guidance for the Information Systems Security (INFOSEC) program per reference (z), and is responsible for Information Management and Information Technology (IM/IT) policies, directives, instructions, and guidance, and approves strategies, architectures, standards, and plans for the Navy and Marine Corps.

4. **The Director, Navy International Programs Office (Navy IPO)** is responsible to the ASN(RD&A) for implementing policies and managing DON participation in international efforts concerning RD&A. The Director makes release determinations for disclosure of classified and controlled unclassified information to foreign governments and organizations in compliance with NDP, and manages certain personnel exchange programs with foreign governments.

5. **The Commandant of the Marine Corps (CMC)** administers the DON ISP within the Marine Corps. Designated functions are performed by specific organizations within the Headquarters, Marine Corps:

a. **CMC (Code ARS)** is responsible for implementation of CI and human intelligence programs.

b. **CMC (Code CIZ)**, as Special Security Officer (SSO) for the Marine Corps, is responsible for guidance and implementation of SCI programs.

6. **The Director of Naval Intelligence (DNI) (CNO (N2))**, as the SOIC of the DON, is responsible for administering SCI programs for the DON. **The Office of Naval Intelligence (ONI)**, under the DNI (CNO (N2)), is responsible for the security management and implementation of SCI programs. **The Director, Security Directorate/SSO Navy (ONI-5)**, is responsible for guidance and instruction on matters concerning the security, control, and utilization of SCI.

7. **The Director, Space, Information Warfare, Command and Control (CNO (N6)), Head, Navy Defensive Information Warfare/Information Systems Security Branch (CNO (N643))**, in coordination with the DON CIO, is responsible for policy, implementation, and oversight of the DON INFOSEC program, and issues reference (aa).

8. **The Director, Special Programs Division (N89)** is designated as the DON SAP coordinator and is responsible for the management of the DON SAP Central Office, and to coordinate SAP approval, administration, support, review, and oversight per references (e), (k), and (l).

9. **The COMNAVSECGRU**, as the designated SSO for the NAVSECGRU, is responsible for signals intelligence activities and for administration of SCI programs within the DON cryptologic community.

10. **The Director, COMSEC Material System (DCMS)** administers the DON CMS program and acts as the central office of records for all DON CMS accounts per references (i) and (ab).

REFERENCES

(a) Executive Order 12958, *Classified National Security Information*, 17 Apr 95

(b) *Office of Management and Budget, Implementing Directive* for E.O. 12958, 32 CFR Part 2001, 13 Oct 95

(c) *Subpart D, "Safeguarding" of Information Security Oversight Office (ISOO) Directive 1*, 25 Jun 82

(d) DoD Directive 5200.1, *DoD Information Security Program*, 13 Dec 96 (NOTAL)

(e) DoD 5200.1-R, *DoD Information Security Program Regulation*, 14 Jan 97 (NOTAL)

(f) Executive Order 12829, *National Industrial Security Program*, 6 Jan 93

(g) DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*, 30 Jun 98 (NOTAL)

(h) *DOE Final Rule on Nuclear Classification and Declassification*, 10 CFR, Part 1045, 22 Dec 97 (NOTAL)

(i) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(j) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(k) DoD Directive 0-5205.7, *Special Access Program (SAP) Policy*, 13 Jan 97 (NOTAL)

(l) DoD Instruction 0-5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, 1 Jul 97

(m) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(n) SECNAVINST S5460.3B, *Control of Special Access Programs Within the Department of the Navy*, 30 Aug 91 (NOTAL)

(o) OPNAVINST S5460.4C, *Control of Special Access Programs Within the Department of the Navy* (U), 14 Aug 81 (NOTAL)

(p) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(q) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(r) Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act* of 30 Aug 54, as amended

(s) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(t) USSAN 1-69, *United States Implementation of NATO Security Procedures*, 21 Apr 82 (NOTAL)

(u) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(v) Title 50, U.S.C., Section 403(g), *National Security Act*

(w) DoD 5200.2-R, *DoD Personnel Security Program Regulation*, 19 Jan 87 (NOTAL)

(x) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(y) DoD Directive 5200.1-M, Acquisition System Protection *Program*, 16 Mar 94 (NOTAL)

(z) SECNAVINST 5239.3, *Department of the Navy Information Systems Security (INFOSEC) Program*, 14 Jul 95 (NOTAL)

(aa) OPNAVINST 5239.1A, *Department of the Navy Automatic Data Processing Security Program*, 3 Aug 82

(ab) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

# CHAPTER 2

# COMMAND SECURITY MANAGEMENT

## 2-1 COMMANDING OFFICER

1. **Terminology.** **"Command"** is used as a generic term for any organizational entity and may include a base, station, unit, laboratory, installation, facility, center, activity, detachment, squadron, ship, etc. **"Commanding officer"** is used throughout this regulation as a generic term for the head of any DON command and includes commander, commanding general, director, officer in charge, etc.

2. **Responsibility and Authority.** The commanding officer is responsible for the effective management of the ISP within the command. Authority delegated by this regulation to a commanding officer may be further delegated unless specifically prohibited.

3. **Standards.** This regulation establishes baseline standards, but the commanding officer may impose more stringent requirements within the command or upon subordinates if the situation warrants. The commanding officer shall not, however, unilaterally establish requirements that impact on other commands or cleared DoD contractors, or that contradict this regulation or reference (a).

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

5. **Implementation.** The commanding officer shall designate, in writing, certain security personnel directly involved in program implementation (see paragraphs 2-2 through 2-9). Additionally, the commanding officer shall:

a. Issue a written command security instruction (see **exhibit 2A**).

b. Approve an emergency plan which includes provisions for the protection and destruction of classified information in emergency situations (see **exhibit 2B**).

c. Establish and maintain a self-inspection program for the command. This may include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command's ISP (see **exhibit 2C**).

d. Establish an industrial security program when the command engages in classified procurement or when cleared DoD contractors operate within areas under their direct control.

e. Apply risk management, as appropriate, for the safeguarding of classified information, and monitor its effectiveness in the command.

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

g. Inform command personnel that they are expected and encouraged to challenge the classification of information which they believe to be improperly classified and ensure that procedures for challenging and appealing such status are understood.

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

## 2-2 SECURITY MANAGER

1. The commanding officer shall designate, in writing, a command security manager. The security manager is responsible for implementing the ISP and shall have direct access to the commanding officer. Some tasks may be assigned to a number of command personnel and may even be assigned to persons senior to the security manager. Nevertheless, the security manager shall remain cognizant of all command information, personnel, and industrial security functions and ensure that the security program is coordinated and inclusive of all requirements in this regulation. The security manager shall:

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

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

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

d. Formulate, coordinate, and conduct the command security education program.

e. Ensure that threats to security, and other security violations are reported, recorded, and, when necessary, investigated. Ensure that incidents described in chapter 12 of this regulation are immediately referred to the nearest NCIS office.

f. Coordinate the preparation and maintenance of security classification guides under the command's cognizance.

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

h. Coordinate with other command officials regarding security measures for the classification, safeguarding, transmission and destruction of classified information.

i. Develop security measures and procedures regarding visitors who require access to classified information.

j. Ensure that classified information is secured and controlled areas are sanitized when a visitor is not authorized access.

k. Implement and interpret, as needed, regulations governing the disclosure of classified information to foreign governments.

l. Ensure compliance with the requirements of this regulation when access to classified information is provided at the command to industry in connection with a classified contract.

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

2. The command security manager may be assigned full-time, part-time or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the previous 5 years.

3. The security manager shall be identified by name on command organizational charts, telephone listings, rosters, or other media. Reference (c) recommends that the security manager report to the commanding officer on functional security matters and to the executive officer for administration of the ISP.

## 2-3 TOP SECRET CONTROL OFFICER (TSCO)

1. The commanding officer shall designate, in writing, a command TSCO for commands handling Top Secret information. A Top Secret Control Assistant(s) (TSCA(s)) may be assigned as needed (see paragraph 2-4.4). The TSCO reports directly to the security manager or the security manager may serve concurrently as the TSCO. The TSCO shall:

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

b. Ensure that inventories of Top Secret information are conducted at least once annually, and more frequently when circumstances warrant (see chapter 7, paragraph 7-3). As an exception, repositories, libraries, or activities which store large volumes of classified documents may limit their annual inventory to that which access has been given in the past 12 months, and 10 percent of the remaining inventory.

2. The TSCO must be an officer, senior non-commissioned officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of an SSBI completed within the previous 5 years.

## 2-4 OTHER SECURITY ASSISTANTS

1. **Assistant Security Manager.** In large commands and where circumstances warrant, the commanding officer shall designate, in writing, a command assistant security manager to assist in program implementation and maintenance. The responsibilities

assigned to assistant security managers shall be commensurate with their grade level and experience, understanding that the security manager will provide the guidance, coordination, and oversight necessary to ensure that the program is being administered effectively.

2. A person designated as an assistant security manager must be a U.S. citizen, and either an officer, enlisted person E-6 or above, or civilian employee GS-6 or above. Assistant security managers must have an SSBI if they are designated to issue interim security clearances; otherwise, the investigative and clearance requirements will be determined by the level of access to classified information required.

3. **Security Assistant.** Civilian and military member employees performing administrative functions under the direction of the security manager may be assigned without regard to rate or grade as long as they have the clearance needed for the access required to perform their assigned duties and taskings.

4. **TSCA(s).** The commanding officer shall designate, in writing, a TSCA(s) to assist the TSCO, as needed. Top Secret couriers are not considered to be TSCA(s).

5. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. An established Top Secret security clearance eligibility is required.

## 2-5 SECURITY RELATED COLLATERAL DUTIES

1. **CMS Custodian.** Reference (d) requires that the commanding officer designate, in writing, a CMS custodian and an alternate to manage COMSEC information issued to a CMS account. The CMS custodian is the commanding officer's primary advisor on matters concerning the security and handling of COMSEC information and the associated records and reports.

2. **Naval Warfare Publications (NWP) Custodian.** Reference (e) requires the commanding officer to designate, in writing, an NWP custodian. This assignment is normally a collateral duty. The NWP custodian receipts and accounts for NWPs, ensures completion of Preliminary Inquiries (PIs) and Judge Advocate General Manual (JAGMAN) investigations for loss or compromised publications, and provides procedures for inclusion in the command emergency action plan.

3. **NATO Control Officer.** The commanding officer shall designate, in writing, a command NATO control officer and at least one alternate to ensure that NATO information is correctly controlled and accounted for, and that NATO security procedures are observed. Reference (f) establishes procedures and minimum security standards for the handling and protection of NATO classified information. The CUSR is the main receiving and dispatching element for NATO information in the U.S. Government. The CUSR manages the U.S. Registry System of subregistries and control points to maintain accountability of NATO classified information.

## 2-6 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The contracting officer shall designate, in writing, one or more qualified security specialists per Subpart 201.602-2 of reference (g), as CORs, previously called "Contracting Officer's Security Representative." The designation shall be for the purpose of signing the Contract Security Classification Specification (DD 254), and revisions thereto. The COR is responsible to the security manager for coordinating with program managers and procurement officials. The COR shall ensure that the industrial security functions specified in chapter 11 are accomplished when classified information is provided to industry for performance on a classified contract.

## 2-7 INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

Per reference (h), the commanding officer shall designate, in writing, an ISSM and Information Systems Security Officer(s) (ISSOs), as appropriate. The ISSM serves as the point of contact for all command INFOSEC matters and implements the command's INFOSEC program. ISSOs are designated for each information system and network in the command responsible for implementing and maintaining the command's information system and network security requirements. In some commands, the ISSM and ISSO duties may be performed by the same person.

## 2-8 SPECIAL SECURITY OFFICER (SSO)

1. Per reference (i), the commanding officer shall designate, in writing, a command SSO and Subordinate Special Security Officer (SSSO), as needed, for any command that is accredited for and authorized to receive, store, and process SCI. The SSO is responsible for the operation (e.g. security, control, use, etc.) of all command Sensitive Compartmented Information Facilities (SCIFs). All SCI matters shall be referred to the SSO. The SSO may be designated as security manager if the grade requirements

for security manager are met; however, the security manager cannot function as an SSO unless designated by the Director, ONI or COMNAVSECGRU.

2. The SSO and the SSSO must be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and must meet the standards of reference (j).

**2-9 SECURITY OFFICER**

Per reference (k), the commanding officer shall designate, in writing, a command security officer. This official may serve concurrently as security manager.

**2-10 SECURITY SERVICING AGREEMENTS (SSAs)**

1. Specified security functions may be performed for other commands via SSAs. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including:

a. A command provides security services for another command, or the command provides services for a tenant activity;

b. A command is located on the premises of another government entity and the host command negotiates an agreement for the host to perform security functions;

c. A senior in the chain of command performs or delegates certain security functions of one or more subordinate commands;

d. A command with a particular capability for performing a security function agrees to perform the function for another;

e. A command is established expressly to provide centralized service (e.g., Personnel Support Activity or Human Resources Office); or

f. When either a cleared contractor or a long term visitor group is physically located at a DON command.

2. The SSA shall be specific and shall clearly define the security responsibilities of each participant. The agreement shall include requirements for advising commanding officers of any matter(s) which may directly affect the security integrity of the command.

## 2-11 INSPECTIONS, ASSIST VISITS, AND PROGRAM REVIEWS

1. Commanding officers are responsible for evaluating the security posture of their subordinate commands.

2. Senior commanders may, as determined necessary, conduct inspections, assist visits, and reviews to examine overall security posture of subordinate commands. Unless otherwise required, it is not necessary to conduct separate inspections for security. They may be conducted during other scheduled inspections and results identified as such (see **exhibit 2C**).

3. Refer to **appendix D** of reference (b) for the PSP inspection checklist.

## 2-12 FORMS

**Appendix B** lists the forms used in the ISP along with purchasing information.

## 2-13 REPORT CONTROL SYMBOLS

**Appendix C** lists the report control symbols required by this regulation.

## REFERENCES

(a) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(b) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(c) OPNAVINST 3120.32C, *Standard Organization and Regulations of the U.S. Navy*, 11 Apr 94 (NOTAL)

(d) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(e) NWP 1-01, *Naval Warfare Publications Systems*, Nov 94 (NOTAL)

(f) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(g) *Defense Federal Acquisition Regulation, Subpart 201.602-2*

(h) OPNAVINST 5239.1A, *Department of the Navy Automatic Data Processing Security Program*, 3 Aug 82

(i) DoD 5105-21-M-1, *DoD Sensitive Compartmented Information Administrative Manual*, 3 Aug 98 (NOTAL)

(j) Director, Central Intelligence Directive (DCID) 1/14, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, 2 Jul 98 (NOTAL)

(k) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98 (NOTAL)

## EXHIBIT 2A

## GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. The security manager shall assess the vulnerability of the command classified information to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified information, mission of the command, countermeasures available and the cost, and the effectiveness of alternative courses of action. Results of this assessment shall be used to develop a command security instruction which will emulate the organization of this regulation and identify any unique command requirements. The command security instruction shall supplement this regulation and other directives from authorities in the command administrative and operational chain.

2. Incorporate the following into the command security instruction:

a. The purpose, applicability, and relationship to other directives, particularly this regulation.

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Cite and append SSAs, if applicable.

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

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

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

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

i. State whether the commanding officer and any other command officials have been delegated Top Secret or Secret original classification authority.

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

k. Develop an industrial security program and identify key personnel, such as the COR, if applicable.

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

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

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

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

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

3. Refer to SECNAVINST 5510.30A for guidance concerning personnel security investigations, adjudications, and clearances.

# EXHIBIT 2B

## EMERGENCY PLAN AND EMERGENCY DESTRUCTION SUPPLEMENT

### PART ONE: EMERGENCY PLAN

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

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

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

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

after the emergency (even though a document-by-document inventory may not be possible under current accountability guidelines).

**PART TWO: EMERGENCY DESTRUCTION SUPPLEMENT**

1. Commands located outside the U.S. and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans (CMS-1A provides additional emergency destruction policy and guidance for commands that handle COMSEC information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of incidents or emergency destruction of classified information shall be reported to the CNO (N09N2).

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

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

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

5. Naval surface noncombatant vessels operating in hostile areas without escort shall have appropriate equipment on board prepared for use.

YES NO N/A

## EXHIBIT 2C

## SECURITY INSPECTION CHECKLIST

### INTRODUCTION TO THE ISP

__ __ __ 1. Does the command hold the current edition of SECNAVINST 5510.36? (1-1)

2. Is the command in possession of the following classified information references: (1-1)

__ __ __ a. COMSEC, CMS-1A/CMS-21?
__ __ __ b. DoD SCI Security Manual/relevant DCIDs?
__ __ __ c SAPs, OPNAVINST S5460.4C?
__ __ __ d. SIOP and SIOP-ESI, OPNAVINST S5511.35K?
__ __ __ e. NNPI, NAVSEAINST C5511.32B?
__ __ __ f. RD/FRD, DoD Directive 5210.2?
__ __ __ g. CNWDI, DoD Directive 5210.2?
__ __ __ h. NATO, OPNAVINST C5510.101D?
__ __ __ i. Classified information released to industry, NISPOM?
__ __ __ j. Controlled unclassified information, DoD 5200.1-R?

__ __ __ 3. Are waivers and exceptions submitted to the CNO (N09N2) for all conditions that prevent compliance with SECNAVINST 5510.36? (1-2)

### COMMAND SECURITY MANAGEMENT

1. Has the commanding officer: (2-1)

__ __ __ a. Issued a command security instruction?
__ __ __ b. Approved an emergency plan for the protection and destruction of classified information?
__ __ __ c. Established an Industrial Security Program?
__ __ __ d. Ensured that the security manager and other personnel have received security education and training?
__ __ __ e. Ensured that personnel are evaluated on the handling, creation or management of classified information on performance evaluations?

| YES | NO | N/A | |
|---|---|---|---|
| | | | 2. To implement the ISP, has the commanding officer designated in writing a command? |
| __ | __ | __ | a. Security manager? (2-2) |
| __ | __ | __ | b. TSCO? (2-3) |
| __ | __ | __ | c. TSCA? (2-3) |
| __ | __ | __ | d. Assistant security manager? (2-4) |
| __ | __ | __ | e. Security assistant(s)? (2-4) |
| __ | __ | __ | f. CMS custodian and alternate? (2-5) |
| __ | __ | __ | g. NWP custodian? (2-5) |
| __ | __ | __ | h. NATO control officer and alternate? (2-5) |
| __ | __ | __ | i. One or more CORs? (2-6) |
| __ | __ | __ | 3. Is the command security manager named and identified to command personnel on command organizational charts, telephone listings, rosters, or other media? (2-2) |
| | | | 4. Has the command security manager: (2-2) |
| __ | __ | __ | a. Developed a command security instruction? |
| __ | __ | __ | b. Formulated, coordinated, and conducted a command security education program? |
| __ | __ | __ | c. Kept command personnel abreast of all changes in security policies and procedures? |
| __ | __ | __ | d. Reported and investigated all security threats and compromises? |
| __ | __ | __ | e. Promptly referred all incidents, under their jurisdiction, to the NCIS? |
| __ | __ | __ | f. Coordinated the preparation of the command SCGs? |
| __ | __ | __ | g. Maintained liaison with the PAO on proposed media releases? |
| __ | __ | __ | h. Developed security procedures for visitors who require access to classified information? |
| __ | __ | __ | i. Implemented regulations concerning the disclosure of classified information to foreign nationals? |
| __ | __ | __ | 5. Does the TSCO manage and control all command TS information, less SCI? (2-3) |

| YES | NO | N/A | |
|---|---|---|---|
| ___ | ___ | ___ | 6. Are security functions performed by another command covered by a written SSA? (2-10) |
| ___ | ___ | ___ | 7. Have qualified security inspectors conducted command inspections, assist visits, and program reviews to examine the command's overall security posture? (2-11) |

**SECURITY EDUCATION**

| | | | |
|---|---|---|---|
| ___ | ___ | ___ | 1. Does the command have an effective information security education program? (3-1) |
| | | | 2. Is additional ISP training provided to? (3-3) |
| ___ | ___ | ___ | a. Approved OCAs? |
| ___ | ___ | ___ | b. Derivative classifiers, security managers, and other security personnel? |
| ___ | ___ | ___ | c. Classified couriers? |
| ___ | ___ | ___ | d. Declassification authorities? |

**CLASSIFICATION MANAGEMENT**

| | | | |
|---|---|---|---|
| ___ | ___ | ___ | 1. Is information classified only to protect NSI? (4-1) |
| ___ | ___ | ___ | 2. Do procedures prohibit the use of terms such as "For Official Use Only" or "Secret Sensitive" for the identification of classified information? (4-2) |
| ___ | ___ | ___ | 3. Have the command OCAs been trained in their duties and responsibilities? (4-6) |
| ___ | ___ | ___ | 4. Has written confirmation of this training (i.e., indoctrination letter) been submitted to the CNO (N09N2)? (4-6) |
| ___ | ___ | ___ | 5. Is information, not officially released or disclosed to the public, classified or reclassified only if the information meets the criteria of E.O. 12958? (4-11) |
| ___ | ___ | ___ | 6. Is the classification level, of any information believed to be improperly classified, challenged? (4-12) |

| YES | NO | N/A | | |
|---|---|---|---|---|
| __ | __ | __ | 7. | Does NATO and FGI retain its original classification level and is it assigned an English classification equivalent, if necessary? (4-17, 6-14) |
| __ | __ | __ | 8. | Are procedures established for the completion of command mandatory declassification reviews within 45 working days? (4-23) |
| __ | __ | __ | 9. | Are reasonable steps taken to declassify information determined to be of permanent historical value prior to their accession into NARA? (4-25) |
| __ | __ | __ | 10. | Have cognizant OCAs notified holders of unscheduled classification changes involving their information? (4-26) |

**SECURITY CLASSIFICATION GUIDES**

| | | | | |
|---|---|---|---|---|
| __ | __ | __ | 1. | Is a SCG issued for each classified system, program, plan, or project before the initial funding or implementation of the system, program, plan, or project? (5-1) |
| __ | __ | __ | 2. | Is each SCG approved personally and in writing by an OCA who has program or supervisory responsibility over the information? (5-2) |
| __ | __ | __ | 3. | Are command SCGs formatted per OPNAVINST 5513.1E? (5-2) |
| __ | __ | __ | 4. | Are command-originated SCGs reviewed, by the cognizant OCA, at least every 5 years? (5-4) |
| __ | __ | __ | 5. | Are all changes promptly submitted to the Rankin Program Manager? (5-4) |

**MARKING**

| | | | | |
|---|---|---|---|---|
| __ | __ | __ | 1. | Are classified documents and their portions properly marked to include all applicable basic and associated markings? (6-1, 6-5) |

| YES | NO | N/A | | |
|---|---|---|---|---|
| __ | __ | __ | 2. | Are originally classified documents marked with a "Classified by" and "Reason" line? (6-8) |
| __ | __ | __ | 3. | Are derivatively classified documents marked with a "Derived from" line? (6-9) |
| __ | __ | __ | 4. | Is "Multiple Sources" annotated on the "Derived from" line of classified documents derived from more than one source? (6-9) |
| __ | __ | __ | 5. | Is a source listing attached to the file copy of all documents classified by "Multiple Sources?" (6-9) |
| __ | __ | __ | 6. | Are downgrading and declassification instructions included on all classified documents, less exception documents? (6-10) |
| __ | __ | __ | 7. | Are the appropriate warning notices placed on the face of classified documents? (6-11) |
| __ | __ | __ | 8. | Are classified intelligence documents/portions marked with the appropriate intelligence control marking(s)? (6-12) |
| __ | __ | __ | 9. | Are the portions of documents containing NATO and FGI marked to indicate their country of origin? (6-14) |
| __ | __ | __ | 10. | Is the face of NATO and foreign government RESTRICTED documents and FGI marked with the appropriate notice? (6-15) |
| __ | __ | __ | 11. | Is the assignment and use of nicknames, exercise terms, and code words per OPNAVINST 5511.37C? (6-17) |
| __ | __ | __ | 12. | Is an explanatory statement included on the face of documents classified by compilation? (6-18) |

YES NO N/A

__ __ __ 13. Do documents, marked classified for training and test purposes, include a statement indicating that the documents are actually unclassified? (6-20)

__ __ __ 14. When removed or used separately, are component parts of classified documents marked as separate documents? (6-21)

__ __ __ 15. Are letters of transmittal marked to show the highest overall classification level of any information being attached or enclosed? (6-24)

__ __ __ 16. Are electronically transmitted messages properly marked? (6-25)

__ __ __ 17. Are classified files or folders marked or have the appropriate SFs been attached to indicate the highest overall classification level of the information contained therein? (6-26)

__ __ __ 18. Are all classified materials such as AIS media, maps, charts, graphs, photographs, slides, recordings, and videotapes appropriately marked? (6-27 through 6-34)

**SAFEGUARDING**

__ __ __ 1. Does the command ensure that all DON employees (military and civilian) who resign, retire, separate, or are released from active duty, return all classified information in their possession? (7-1)

__ __ __ 2. Is TS information including copies, originated or received by the command, continuously accounted for, individually serialized, and entered into the command's TS inventory? (7-3)

__ __ __ 3. Are command TS documents and material physically sighted at least annually? (7-3)

__ __ __ 4. Does the command have control measures in place for the receipt and dispatch of Secret information? (7-4)

| YES | NO | N/A | | |
|---|---|---|---|---|
| — | — | — | 5. | Are control measures in place to protect unauthorized access to command TS, Secret, or Confidential information? (7-3, 7-4, 7-5) |
| | | | 6. | Are working papers: (7-6) |
| — | — | — | | a. Dated when created? |
| — | — | — | | b. Marked "Working Paper" on the first page? |
| — | — | — | | c. Marked with the highest overall classification, center top and bottom, of each applicable page? |
| — | — | — | | d. Destroyed when no longer needed? |
| — | — | — | | e. Brought under accountability after 180 days or when they are released outside the command? |
| — | — | — | 7. | Are appropriate control measures taken for other special types of classified information? (7-7) |
| — | — | — | 8. | Are SFs 703, 704, and 705 placed on all classified information when removed from secure storage? (7-9) |
| — | — | — | | a. Are SFs 706, 707, 708, and 712 being utilized on all classified AIS media? |
| — | — | — | | b. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level? |
| — | — | — | 9. | Has the command established procedures for end of day security checks, to include the use of SFs 701 and 702? (7-10) |
| — | — | — | 10. | Are classified vaults, secure rooms, and containers made an integral part of the end of day security check? (7-10) |
| — | — | — | 11. | Are procedures in place to ensure that visitors have access only to information for which they have a need-to-know and the appropriate clearance level? (7-11) |

| YES | NO | N/A | |
|---|---|---|---|
| __ | __ | __ | 12. Are procedures in place for classified meetings held at the command or hosted at cleared facilities? (7-12) |
| __ | __ | __ | 13. Is classified information reproduced only to the extent that is mission essential? (7-13) |

**DISSEMINATION**

| | | | |
|---|---|---|---|
| __ | __ | __ | 1. Are procedures established to ensure the proper dissemination of classified information outside DoD and to foreign governments? (8-1) |
| __ | __ | __ | 2. Are special types of classified and controlled unclassified information disseminated per their governing instructions? (8-4) |
| __ | __ | __ | 3. Is information disseminated to Congress per SECNAVINST 5730.5 and OPNAVINST 5510.158? (8-6) |
| __ | __ | __ | 4. Do all newly generated classified and unclassified technical documents include a distribution statement listed in **exhibit 8A** of SECNAVINST 5510.36? (8-7) |
| __ | __ | __ | 5. Are all DoD-funded RDT&E programs that involve Navy scientific and technical information and unclassified technical data that reveal critical technology disseminated per their applicable instruction? (8-7) |
| __ | __ | __ | 6. Is command information intended for public release, including information released through AIS means (i.e., INTERNET, computer servers), submitted for prepublication review? (8-8) |

**TRANSMISSION AND TRANSPORTATION**

| | | | |
|---|---|---|---|
| __ | __ | __ | 1. Is classified information transmitted and transported only per specific requirements? (9-2, 9-3, 9-4) |

| YES | NO | N/A | |
|---|---|---|---|
| 17 MAR 1999 | | | |
| __ | __ | __ | 2. Are special types of classified information transmitted and transported per their governing instructions? (9-5) |
| __ | __ | __ | 3. Are command personnel advised not to discuss classified information over unsecured circuits? (9-6) |
| __ | __ | __ | 4. Are command procedures established for preparing classified bulky shipments as freight? (9-7) |
| __ | __ | __ | 5. Is classified information transported or transmitted outside the command receipted for? (9-10) |
| __ | __ | __ | 6. Does the command authorize the handcarry or escort of classified information, via commercial aircraft, only if other means are not available, and there is an operational need or contractual requirement? (9-11) |
| __ | __ | __ | 7. Are designated couriers briefed on their courier responsibilities and requirements? (9-11) |
| __ | __ | __ | 8. Are procedures established for the control and issuance of the DD 2501? (9-12) |

**STORAGE AND DESTRUCTION**

| | | | |
|---|---|---|---|
| __ | __ | __ | 1. Are any command weaknesses, deficiencies, or vulnerabilities in any equipment used to safeguard classified information reported to the CNO (N09N3)? (10-1) |
| __ | __ | __ | a. Does the command ensure that weapons, money, jewelry or narcotics are not stored in security containers used to store classified information? |
| __ | __ | __ | b. Does the command ensure that external markings on command security containers do not reveal the level of information stored therein? |

| YES | NO | N/A | |
|---|---|---|---|
| ___ | ___ | ___ | 2. Does command security equipment meet the minimum standards of GSA? (10-2) |
| ___ | ___ | ___ | 3. Does the command meet the requirements for the storage of classified bulky information? (10-3) |
| ___ | ___ | ___ | 4. Does the command mailroom have a GSA-approved security container to store USPS first class, certified, and registered mail overnight? (10-3) |
| ___ | ___ | ___ | 5. Are command vaults and secure rooms, not under visual control at all times during duty hours, equipped with electric, mechanical, or electro-mechanical access control devices? (10-7) |
| ___ | ___ | ___ | 6. Are specialized security containers securely fastened to the structure, rendering them non-portable? (10-8) |
| ___ | ___ | ___ | 7. Has the command removed all containers manufactured by Remington Rand? (10-9) |
| ___ | ___ | ___ | 8. Is classified information removed from designated work areas for work at home done so only with prior approval of appropriate officials? (10-10) |
| | | | 9. Are command container combinations changed: (10-12) |
| ___ | ___ | ___ | a. By individuals who possess the appropriate clearance level? |
| ___ | ___ | ___ | b. Whenever the container is first put into use? |
| ___ | ___ | ___ | c. Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)? |
| ___ | ___ | ___ | d. Whenever a combination has been subjected to compromise? |
| ___ | ___ | ___ | e. Whenever the container is taken out of service? |

| YES | NO | N/A | | |
|---|---|---|---|---|
| __ | __ | __ | 10. | Are command container combinations marked, and accounted for per the classification level of the information stored therein? (10-12) |
| __ | __ | __ | 11. | Is there an SF 700 affixed inside each command security container? (10-12) |
| __ | __ | __ | 12. | Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination? (10-12) |
| __ | __ | __ | 13. | Has the command established procedures for command key and padlock accountability and control? (10-13) |
| __ | __ | __ | 14. | Are command locks repaired only by authorized personnel who have been subject to a trustworthiness determination or who are continuously escorted? (10-15) |
| __ | __ | __ | 15. | Are command security containers, previously placed out of service, marked as such on the outside and the "Test Certification Label" removed on the inside? (10-15) |
| __ | __ | __ | 16. | Are command security containers, with visible repair results, marked as such with a label posted inside the container stating the details of the repairs? (10-15) |
| __ | __ | __ | 17. | Are all commercial IDSs used on command security containers, vaults, modular vaults, and secure rooms approved by the CNO (N09N3)? (10-16) |
| __ | __ | __ | 18. | Is command classified information destroyed when no longer required? (10-17) |
| __ | __ | __ | 19. | Do all command shredders, pulverizers, and disintegrators meet the minimum requirements? (10-18) |
| __ | __ | __ | 20. | Has the command established effective procedures for the destruction of classified information? (10-19) |

YES NO N/A

___ ___ ___ 21. When filled, are command burn bags sealed and safeguarded per the highest overall classification level of their contents? (10-19)

___ ___ ___ 22. Is controlled unclassified information destroyed per the governing instructions? (10-20)

**INDUSTRIAL SECURITY PROGRAM**

___ ___ ___ 1. Has the command established an Industrial Security Program? (11-1)

___ ___ ___ 2. Has the command developed a PPP? (11-1)

___ ___ ___ 3. Has the commanding officer established or coordinated oversight over classified work carried out by cleared DoD contractor employees in spaces controlled or occupied at DON shore commands? (11-5)

___ ___ ___ 4. Have all FADs been issued per SECNAVINST 5510.30A? (11-6)

5. Does the command COR: (11-8)

___ ___ ___ a. Complete, issue, and sign all DD 254s?
___ ___ ___ b. Validate all contractor security clearances?
___ ___ ___ c. Verify FCLs and storage capability prior to release of classified information?
___ ___ ___ d. Certify and approve all DD 1540s?
___ ___ ___ e. Provide additional security requirements?
___ ___ ___ f. Review all reports of industry security violations and forward to program managers?
___ ___ ___ g. Coordinate DD 254 reviews and guidance, as needed?
___ ___ ___ h. Verify that cleared DoD contractor employees who are used as couriers have been briefed on their courier responsibilities? (11-12)

| YES | NO | N/A | |
|---|---|---|---|
| __ | __ | __ | 6. Is classified intelligence information disclosed only to those contractors cleared under the NISP? (11-14) |

**LOSS OR COMPROMISE OF CLASSIFIED INFORMATION**

| | | | |
|---|---|---|---|
| __ | __ | __ | 1. Since the last inspection, has the command had any incidents involving a loss or compromise of classified information? (12-1) |
| __ | __ | __ | 2. If a possible loss or compromise occurred, was a PI conducted? (12-4) |
| __ | __ | __ | 3. If a significant command weakness is identified, or a confirmed loss or compromise occurred, was a JAGMAN investigation conducted? (12-9) |
| __ | __ | __ | 4. When a loss or compromise of classified information or equipment has occurred, is appropriate investigative and remedial action(s) taken to ensure further loss or compromise does not recur? (12-14) |
| __ | __ | __ | 5. Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent compromise or repeated administrative disregard of security regulations occurs? (12-14) |
| __ | __ | __ | 6. Are procedures established for review of investigations by seniors? (12-14) |
| __ | __ | __ | 7. Are security reviews conducted on information subjected to loss or compromise? (12-15) |
| __ | __ | __ | 8. Are procedures established for classification reviews by originators or OCAs? (12-16) |
| __ | __ | __ | 9. Is receipt of improperly transmitted information reported to the sender? (12-19) |

# CHAPTER 3

# SECURITY EDUCATION

## 3-1 BASIC POLICY

Commanding officers shall ensure that personnel in their commands receive the security education necessary to enable quality performance of their security functions.

## 3-2 RESPONSIBILITY

The CNO (N09N) is responsible for policy guidance, education requirements and support for the DON security education program (see chapter 4 of reference (a) for detailed guidance concerning the execution of the DON's security education program).

## 3-3 ADDITIONAL INFORMATION SECURITY EDUCATION

1. In addition to the security education requirements of reference (a), specialized training is required for the following:

a. Original Classification Authorities (OCAs) (see chapter 4, paragraph 4-4);

b. Derivative classifiers (see chapter 4, paragraph 4-9), security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information;

c. Classified couriers (see chapter 9, paragraph 9-11.5);

d. Declassification authorities (see chapter 4, paragraph 4-19).

## REFERENCE

(a) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

# CHAPTER 4

# CLASSIFICATION MANAGEMENT

## 4-1 BASIC POLICY

1. Reference (a) is the only basis for classifying NSI, except as provided by reference (b). It is DON policy to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information shall be classified only to protect the national security.

2. Information classified by DON Original Classification Authorities (OCAs) (see exhibit 4A) shall be declassified as soon as it no longer meets the standards for classification in the interest of the national security.

## 4-2 CLASSIFICATION LEVELS

1. Information that requires protection against unauthorized disclosure in the interest of national security shall be classified at the Top Secret, Secret, or Confidential levels. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information. Terms such as "For Official Use Only" (FOUO) or "Secret Sensitive" (SS) shall not be used for the identification of U.S. classified information.

2. **Top Secret** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to the national security. Examples include information whose unauthorized release could result in armed hostilities against the U.S. or its allies; a disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans; the disclosure of complex cryptographic and communications intelligence systems; the disclosure of sensitive intelligence operations; and the disclosure of significant scientific or technological developments vital to national security.

3. **Secret** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **serious damage** to the national security. Examples include information whose unauthorized release could result in the disruption of foreign relations significantly affecting the national security; the significant impairment of a program or policy directly related to the national security; the disclosure of significant military plans or intelligence operations; and the

disclosure of scientific or technological developments relating to national security.

4. **Confidential** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to **cause damage** to the national security. Examples include information whose unauthorized release could result in disclosure of ground, air, and naval forces (e.g., force levels and force dispositions); or disclosure of performance characteristics, such as design, test, and production data of U.S. munitions and weapon systems.

## 4-3 ORIGINAL CLASSIFICATION

Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure. This decision shall be made only by persons (i.e., OCAs) who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information.

## 4-4 ORIGINAL CLASSIFICATION AUTHORITY

The authority to originally classify information as Top Secret, Secret, or Confidential rests with the SECNAV and officials delegated the authority. The SECNAV personally designates certain officials to be Top Secret OCAs. The authority to originally classify information as Secret or Confidential is inherent in Top Secret original classification authority. The SECNAV authorizes the CNO (N09N) to designate certain officials as Secret OCAs. The authority to originally classify information as Confidential is inherent in Secret original classification authority. OCAs are designated by virtue of their position. Original classification authority is not transferable and shall not be further delegated. Only the current incumbents of the positions listed in **exhibit 4A** have original classification authority. Periodic updates to **exhibit 4A** can be found on the CNO (N09N2) **Homepage at www.navysecurity.navy.mil.**

## 4-5 REQUESTS FOR ORIGINAL CLASSIFICATION AUTHORITY

1. Submit in writing requests for original classification authority to the CNO (N09N). Each request shall identify the prospective OCA's position and/or title, organization, and justification for original classification authority. Requests for original classification authority shall be granted only when:

a. Original classification is required during the normal course of operations in the command;

b. Sufficient expertise and information is available to the prospective OCA to permit effective classification decision making;

c. The need for original classification cannot be eliminated by issuance of classification guidance by existing OCAs; and

d. Referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical.

## 4-6 OCA TRAINING

All OCAs shall be trained in the fundamentals of security classification, the limitations of their classification authority, and their OCA duties and responsibilities. This training is a prerequisite for an OCA to exercise this authority. OCAs shall provide written confirmation (i.e., indoctrination letter) to the CNO (N09N2) that this training has been accomplished. Training shall consist of a review of pertinent E.O.s, statutes, and DON regulations. The CNO (N09N2) will provide OCA training material upon request.

## 4-7 ORIGINAL CLASSIFICATION CRITERIA, PRINCIPLES, AND CONSIDERATIONS

A determination to originally classify shall be made by an OCA only when the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security. Reference (c) contains the specific criteria, principles, and considerations for original classification.

## 4-8 DURATION OF ORIGINAL CLASSIFICATION

1. At the time of original classification, the OCA shall attempt to establish a specific date or event for declassification based upon reference (a) criteria. The date or event shall not exceed 10 years from the date of the original classification.

2. OCAs may exempt certain information from the 10-year maximum duration of classification rule provided the information requires classification past 10 years and falls into one of eight exemption categories ("X1" through "X8," also referred to as "X" codes). The eight categories include that information which would:

a. Reveal an intelligence source, method, or activity, or cryptologic system or activity ("X1");

b. Reveal information that would assist in the development or use of weapons of mass destruction ("X2");

c. Reveal information that would impair the development or use of technology within a U.S. weapons system ("X3");

d. Reveal U.S. military plans, or national security emergency preparedness plans ("X4");

e. Reveal foreign government information (FGI) ("X5");

f. Damage relations between the U.S. and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years ("X6");

g. Impair the ability of responsible U.S. Government officials to protect the President, Vice President, and other individuals for whom protective services, in the interest of national security, are authorized ("X7"); or

h. Violate a statute, treaty, or international agreement ("X8").

3. In the unlikely event an OCA cannot determine a specific date or event for declassification and an "X" code is inappropriate, the information shall be marked for declassification 10 years from the date of the original classification decision (hereafter referred to as the "10-year rule").

4. If information has been assigned a date or event for declassification under the 10-year rule, but the cognizant OCA later has reason to believe longer protection is required, the OCA may extend the classification for successive periods not to exceed 10 years consistent with reference (a) criteria. However, before extending classification, OCAs shall consider their ability and responsibility to notify all holders of this classification extension.

## 4-9 DERIVATIVE CLASSIFICATION

1. While original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, derivative classification is the incorporating, paraphrasing, restating, or

generating, in new form, information that is already classified, and the marking of newly developed information consistent with the classification markings that apply to the classified source. This includes the classification of information based on classification guidance or source documents, but not the mere duplication or reproduction of existing classified information. An estimated 99 percent of the classified information produced by DON commands is derivatively classified.

2. A derivative classifier shall:

a. Observe and respect the original classification determinations made by OCAs (and as codified in classified source documents and security classification guides);

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

c. Carry forward to any newly created information, the pertinent classification markings.

**4-10 ACCOUNTABILITY OF CLASSIFIERS**

Original and derivative classifiers are accountable for the accuracy of their classification decisions. Officials with command signature authority shall ensure that classification markings are correct. Commanding officers may delegate the authority to approve derivative classification decisions to the command security manager.

**4-11 LIMITATIONS ON CLASSIFYING**

1. Information previously declassified and officially released to the public (i.e., disclosed under proper authority) shall not be reclassified.

2. Information not officially released may be classified or reclassified by a Top Secret OCA after a request for it under references (d) or (e) or the mandatory declassification review provision of paragraph 4-23. However, this can occur only if such classification meets the requirements of reference (a), and is accomplished on a document-by-document basis with the personal participation or under the direction of the CNO (N09N).

3. Classifiers shall not:

a. Use classification to conceal violations of law, inefficiency, or administrative error;

b. Classify information to prevent embarrassment to a person, organization, or agency;

c. Classify information to restrain competition;

d. Classify information to prevent or delay the release of information that does not require protection in the interest of national security;

e. Classify basic scientific research information not clearly related to the national security;

f. Classify a product of non-Governmental research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access, unless the U.S. Government acquires a proprietary interest in the product. This prohibition does not affect the provisions of reference (f), (see paragraph 4-15); or

g. Classify, or use as a basis for classification, references to classified documents, when the reference citation does not itself disclose classified information.

**4-12 CLASSIFICATION CHALLENGES**

1. Authorized holders of classified information are encouraged and expected to challenge the classification of information which they, in good faith, believe to be improperly classified.

2. When reason exists to believe information is improperly classified, the command security manager, where the information originated, or the classifier of the information shall be contacted to resolve the issue.

3. If a formal challenge to classification is appropriate, the challenge shall be submitted, via the chain of command, to the OCA. The challenge shall include a sufficient description of the information (i.e., the classification of the information, its classifier or responsible OCA, and reason(s) the information is believed to be improperly classified), to permit identification of the information. The information in question shall be safeguarded as required by its stated classification level until a final decision is reached on the challenge. The OCA shall act

upon a challenge within 30 days of receipt and notify the challenger of any changes made as a result of the challenge or the reason(s) no change is being made.

4. If the person initiating the challenge is not satisfied with the OCA's final determination, the decision may be appealed to the CNO (N09N) for review as the DON's impartial official. If, after appeal to the CNO (N09N), the challenger is still not satisfied, the decision may be further appealed to the Interagency Security Classification Appeals Panel (ISCAP), established by Section 5.4 of reference (a).

5. These procedures do not apply to or affect the mandatory declassification review actions described in paragraph 4-23.

**4-13 RESOLUTION OF CONFLICTS BETWEEN OCAs**

1. Disagreements between two or more DON OCAs shall be resolved promptly. Normally, mutual consideration of the other party's position will provide an adequate basis for agreement. If agreement cannot be reached, the matter shall be referred to the next senior with original classification authority. If agreement cannot be reached at that level, the matter shall be referred for decision to the CNO (N09N) who shall arbitrate the matter.

2. Action on resolution of conflicts shall not take more than 30 days at each level of consideration. Conflicts shall automatically be referred to the next higher echelon if not resolved within 30 days.

3. Holders of the information in conflict shall protect the information at the higher classification level until the conflict is resolved.

**4-14 TENTATIVE CLASSIFICATION**

1. Over classification of information shall be avoided. If there is a reasonable doubt about the need to classify information, it shall not be classified.

2. Individuals, not having original classification authority, who create information they believe to be classified, or which they have significant doubt about the appropriate classification level, shall mark the information at the lower level and:

a. Safeguard the information required for the level of classification;

b. Mark the first page and/or cover sheet of information as tentatively classified with the intended classification level preceded by the word "TENTATIVE" (e.g. "TENTATIVE SECRET"); and

c. Forward the information through the chain of command to the next senior with original classification authority. Include in the body of the transmittal a statement that the information is "tentatively" marked to protect it in transit, and include a justification for the tentative classification.

3. The OCA shall make the classification determination within 30 days.

4. After the OCA's determination, the "TENTATIVE" marking shall be removed and the information shall be remarked to reflect the OCA's decision.

**4-15 PATENT SECRECY INFORMATION**

1. Although only official information shall be classified, there are some circumstances in which information not meeting the definition in paragraph 4-2 may warrant protection in the interest of national security. These circumstances may include those in paragraphs 4-16 through 4-18.

2. Reference (f) provides that the SECDEF, among others, may determine whether granting a patent disclosure for an invention would be detrimental to national security. The SECNAV has been delegated the authority to make determinations on behalf of the SECDEF on matters under the DON cognizance. The Chief of Naval Research (CNR) (Code 300) is the Patent Counsel for the DON and is responsible for making these determinations. When a determination is made, the Commissioner of Patents, at the request of the CNR, takes specified actions concerning the granting of a patent and protection of the information.

**4-16 INDEPENDENT RESEARCH AND DEVELOPMENT INFORMATION (IR&D)/ BID AND PROPOSAL (B&P)**

1. Information that is a product of contractor or individual IR&D/B&P efforts, conducted without prior access to classified information, and associated with the specific information in question, shall not be classified unless:

a. The U.S. Government first acquires a proprietary interest in the information; or

b. The contractor conducting the IR&D/B&P requests that the U.S. Government activity place the information under the control of the security classification system without relinquishing ownership of the information.

2. The individual or contractor conducting an IR&D/B&P effort, and believing that information generated without prior access to classified information or current access to classified information associated with the specific information in question may require protection in the interest of national security, shall safeguard the information and submit it to an appropriate U.S. Government activity for a classification determination. The information shall be marked with a "tentative" classification pending a classification determination (see paragraph 4-14).

a. The U.S. Government activity receiving such a request shall provide security classification guidance or refer the request to the appropriate U.S. Government activity OCA. The information shall be safeguarded until the matter has been resolved.

b. The activity that holds the classification authority over the information shall verify with the Defense Security Service (DSS)/Operations Center Columbus (OCC) whether the individual or contractor is cleared and has been authorized storage capability. If not, the appropriate U.S. Government activity shall advise whether clearance action should be initiated.

c. If the contractor or its employees refuse to be processed for a clearance and the U.S. Government does not acquire a proprietary interest in the information, the information shall not be classified.

**4-17 FOREIGN GOVERNMENT INFORMATION (FGI)**

1. Information classified by a foreign government or international organization retains its original classification level or is assigned a U.S. classification equivalent (see exhibit 6C) to that provided by the originator to ensure adequate protection of the information. Authority to assign the U.S. classification equivalent does not require original classification authority.

2. Foreign Government Unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence shall be classified Confidential. It may be classified at a higher level if it meets the damage criteria of paragraph 4-2.

## 4-18 NAVAL NUCLEAR PROPULSION INFORMATION (NNPI)

1. New projects and significant technical developments or trends related to NNPI are normally classified in order to protect the strategic value of this technology. Classified information related to the tactical characteristics and capabilities of naval nuclear ships and propulsion plant design is typically NSI while classified information relating primarily to the reactor plant of a nuclear propulsion system is typically RD. (The foregoing is a general principle and the specific security classification guides shall be consulted to determine the exact classification levels for specific elements of information).

2. Reference (g) provides detailed guidance for classifying NNPI. The Commander, Naval Sea Systems Command (SEA-08), as the Program Manager for the Naval Nuclear Reactor Program, issues bulletins amplifying or modifying classification and security guidance pertaining to NNPI. These bulletins are disseminated to activities engaged in the Naval Nuclear Propulsion Program and reflect changes, additions, or deletions to the classification guidance in reference (g). General classification guidance, which can in specific instances apply to NNPI, may also be found in references (h) through (l).

## 4-19 AUTHORITY TO DOWNGRADE, DECLASSIFY, OR MODIFY CLASSIFIED INFORMATION

1. The only officials authorized to downgrade, declassify, or modify an original classification determination with a resulting change in the classification guidance for classified DON information are:

a. The SECNAV with respect to all information over which the DON exercises final classification authority;

b. The DON OCA who authorized the original classification, if that official is still serving in the same position;

c. The DON OCA's current successor in function; or

d. A supervisory official of either b or c above, provided that official is a DON OCA.

2. The authority to downgrade, declassify, or modify is not to be confused with the responsibility of an authorized holder of the classified information to downgrade, declassify, or modify it as directed by classification guidance or the relevant OCA.

## 4-20 DECLASSIFICATION BY THE DIRECTOR OF THE ISOO

If the Director of the ISOO determines that information is classified in violation of reference (a), the OCA that originally classified the information may be directed to declassify it. Any such decision may be appealed to the President, through the Assistant to the President for National Security Affairs, via the CNO (N09N). The information shall remain classified pending a decision on the appeal. This provision shall also apply to commands that, under the terms of reference (a), do not have original classification authority, but had such authority under predecessor orders.

## 4-21 AUTOMATIC DECLASSIFICATION

1. Detailed policy concerning the automatic declassification of DON information is contained in reference (m).

2. Reference (a) established procedures for automatic declassification of information in permanently-valuable records (as defined by reference (n)) 25 years from the date of original classification. Automatic declassification shall be applied to existing records over a 5-year period beginning with the date of reference (a) (i.e., 17 April 1995), and shall apply after that to all permanently-valuable records as they become 25 years old. Only the SECDEF and the Secretaries of the Military Departments may exempt information from this automatic declassification provision.

## 4-22 SYSTEMATIC DECLASSIFICATION REVIEW

1. Systematic declassification review is the review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value per chapter 33 of reference (n).

2. The CNO (N09N) is responsible for identifying to the Archivist of the U.S. that classified DON information which is 25 years old and older which still requires continued protection. This includes permanently-valuable records exempted from automatic declassification under Section 3.4 of reference (a). In coordination with the DON OCAs, the CNO (N09N) has developed classification guidelines to be used by the Archivist in reference (m).

3. Special procedures for systematic review for declassification of classified cryptologic information are established by the SECDEF.

4. The DCI may establish procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

5. None of these provisions apply to the systematic review of information classified per reference (b), (RD and FRD).

6. FGI shall not be declassified unless specified or agreed to by the foreign government.

**4-23 MANDATORY DECLASSIFICATION REVIEW**

1. Mandatory declassification is the review for declassification of classified information in response to a request that meets the requirements under Section 3.6 of reference (a). Mandatory declassification review does not supplement or modify the procedures for the handling of FOIA requests as described in reference (d).

2. All information classified under reference (a) or predecessor orders shall be subject to a review for declassification by the DON if:

a. The request for a review describes the information with sufficient specificity to enable its location with a reasonable amount of effort;

b. The information is not exempted from search and review under reference (o);

c. The information has not been reviewed within the preceding 2 years.

3. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, requestors shall be notified and advised of appeal rights.

4. Mandatory declassification requests shall be processed as follows:

a. Command action on the initial request shall be completed within 45 working days.

b. Receipt of each request shall be promptly acknowledged. If no determination has been made within 45 working days of receipt of the request, the requester shall be notified of the right to appeal to the ISCAP, via the CNO (N09N).

c. A determination shall be made whether, under the declassification provisions of reference (a), the requested information may be declassified. If the information is declassified, it shall be provided to the requester unless withholding is otherwise warranted under applicable law. If the information is not releasable in whole or in part, the requester shall be provided a brief statement as to the reason(s) for denial, and notice of the right to appeal within 45 working days. Appeals shall be addressed to the CNO (N09N). A final determination on the appeal shall be made within 30 working days after receipt.

d. Refer requests for declassification involving information originally classified by another DoD Component or U.S. Government agency to that component or agency, when practicable. The requester shall be notified of the referral, unless the request becomes classified due to the association of the information with the originating agency.

5. Refusal to confirm the existence or nonexistence of information is prohibited, unless the fact of its existence or nonexistence can result in damage to the national security.

6. Fees may be charged for mandatory declassification reviews under reference (p), per reference (q). The command can calculate the anticipated amount of fees, and ascertain the requestor's willingness to pay the allowable charges as a precondition before taking further action on the request.

**4-24 INFORMATION EXEMPTED FROM MANDATORY DECLASSIFICATION REVIEW**

Information originated by the incumbent President; the incumbent President's White House Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from mandatory declassification review. The Archivist, however, has the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist per reference (n).

**4-25 CLASSIFIED INFORMATION TRANSFERRED TO THE DON**

1. Classified information officially transferred to the DON in conjunction with a transfer of functions, and not merely for storage purposes, shall become the possession of the DON. The commanding officer of the DON command to which the information is officially transferred shall be considered the downgrading and

declassification authority over the information. If the commanding officer is not a designated downgrading and declassification authority identified in paragraph 4-19, the next senior official in the chain of command, designated the authority, shall review the information for possible downgrading or declassification.

2. Classified information that originated in an agency(ies) or command(s) that have ceased to exist (and for which there is no successor command) shall become the possession of the custodial DON command and may be downgraded or declassified after consultation with any other agency(ies) or command(s) interested in the subject matter. If a determination is made that another agency(ies) or command(s) may have an interest in the continued classification of the information, the custodial DON command shall notify the agency(ies) or command(s) of its intention to downgrade or declassify the information. Notification shall be made to the custodial command within 60 days of any objections concerning the downgrading or declassification of the information; however, the final decision shall reside with the custodial DON command.

3. Before they are accessioned into the National Archives and Records Administration (NARA), OCAs shall take reasonable steps to declassify classified information contained in records determined to be of permanent historical value. The Archivist can require that these records be accessioned into the NARA when necessary to comply with the provisions of reference (n). This provision does not apply to records being transferred to the Archivist under Section 2203 of reference (n), or records for decommissioned commands to which the NARA serves as custodian.

**4-26 NOTIFICATION OF CLASSIFICATION CHANGES**

1. OCAs are responsible for notifying holders of any classification changes involving their information. Original addressees shall be notified of an unscheduled classification change such as classification duration, or a change in classification level.

2. Notices that assign classification to unclassified information shall be classified Confidential, unless the notice itself contains information at a higher classification level. The notice shall be marked for declassification no less than 90 days from its origin. Notices are not issued for information marked with specific downgrading and declassification instructions.

## 4-27 FOREIGN RELATIONS SERIES

The Department of State (DOS) editors of Foreign Relations of the U.S. have a mandated goal of publishing 20 years after the event. Commanding officers shall assist the editors by allowing access to appropriate classified information in their possession and by expediting declassification review of items selected for possible publication.

### REFERENCES

(a) Executive Order 12958, *Classified National Security Information*, 17 Apr 95

(b) Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act* of 30 Aug 54, as amended

(c) OPNAVINST 5513.1E, *DON Security Classification Guides*, 16 Oct 95

(d) SECNAVINST 5720.42E, *DON Freedom of Information Act (FOIA) Program*, 5 Jun 91

(e) Title 5, U.S.C., Section 552a (Public Law 93-579), *The Privacy Act of 1974*

(f) Title 35, U.S.C., Section 181-188, *The Patent Secrecy Act of 1952*

(g) CG-RN-1 (Rev. 3), *DOE-DoD Classification Guide for the Naval Nuclear Propulsion Program (U)*, Feb 96 (NOTAL)

(h) OPNAVINST S5513.3B, *DON Security Classification Guide for Surface Warfare Programs (U)*, 6 Nov 84 (NOTAL)

(i) OPNAVINST S5513.5B, *DON Security Classification Guide for Undersea Warfare Programs (U)*, 25 Aug 93 (NOTAL)

(j) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(k) SECNAVINST 5510.34, *Manual for the Disclosure of DON Military Information to Foreign Governments and International Organizations*, 4 Nov 93

(l) NAVSEAINST 5510.6, *Photographs of U.S. Naval Nuclear Powered Ships and Nuclear Support Facilities; Security Review of*, 6 Mar 75 (NOTAL)

(m) OPNAVINST 5513.16A, *Declassification of 25-Year Old DON Information*, 8 Apr 96 (NOTAL)

(n) Title 44, U.S.C., Chapters 21, 31 and 33, *Federal Records Act*

(o) Title 50, U.S.C., Section 401, *Central Intelligence Agency Information Act*

(p) Title 31, U.S.C., Section 9701 (Title 5 *Independent Offices Appropriation Act*)

(q) NAVSO P1000, *Navy Comptroller Manual, Vol III Procedures*, 21 Apr 98 (NOTAL)

# EXHIBIT 4A

## DEPARTMENT OF THE NAVY
## ORIGINAL CLASSIFICATION AUTHORITIES

| | LEVEL |
|---|---|
| **Office of the Secretary of the Navy** | |
| Secretary of the Navy | TS |
| Under Secretary of the Navy | TS |
| **The General Counsel** | |
| General Counsel of the Navy | TS |
| **Senior Security Official for the Department of the Navy** | |
| Special Assistant for Naval Investigative Matters and Security (N09N)/Director, Naval Criminal Investigative Service | TS |
| **Office of the Judge Advocate General** | |
| Judge Advocate General (00) | S |
| **Assistant Secretary of the Navy** | |
| Assistant Secretary of the Navy (Research, Development and Acquisition) | TS |
| **Department of the Navy Program Executive Officers** | |
| Program Executive Officer for Air ASW, Assault, Special Mission Programs (PEO-A) | TS |
| Program Executive Officer, Cruise Missiles and Joint Unmanned Aerial Vehicles (PEO-CU) | TS |
| Program Executive Officer, Submarines (PEO-SUB) | S |

| | |
|---|---|
| Program Executive Officer, Tactical Aircraft Programs (PEO-T) | TS |
| Program Executive Officer for Undersea Warfare (PEO-USW) | TS |
| Program Executive Officer, Theater Air Defense/Surface Combatants (PEO-TSC) | S |
| Program Executive Officer for Carriers (PEO-CARRIERS) | S |
| Program Executive Officer for DD21 (PEO-DD21) | S |
| Program Executive Officer for Expeditionary Warfare (PEO-EXW) | S |
| Program Executive Officer for Mine Warfare (PEO-MIW) | S |

<u>Chief of Naval Research</u>

| | |
|---|---|
| Chief of Naval Research (00) | TS |
| Commanding Officer, Naval Research Laboratory (1000) | TS |

<u>Naval Air Systems Command</u>

| | |
|---|---|
| Commander, Naval Air Systems Command (AIR-00) | TS |
| Vice Commander, Naval Air System Command (AIR-09) | S |
| Deputy Commander for Acquisition and Operations (AIR-09) | S |
| Assistant Commander for Logistics (AIR-3.0) | S |
| Assistant Commander for Research and Engineering (AIR-4.0) | S |
| Commander, Naval Air Warfare Center, Weapons Division, China Lake, CA (00) | TS |
| Executive Director for Research and Development, Naval Air Warfare Center, Weapons Division, China Lake, CA | S |

**Naval Sea Systems Command**

| | |
|---|---|
| Commander, Naval Sea Systems Command (00) | TS |
| Deputy Commander, Engineering Directorate (03) | S |
| Commanding Officer, Coastal Systems Center, Dahlgren Division, Panama City, FL | S |

**Space and Naval Warfare Systems Command**

| | |
|---|---|
| Commander, Space and Naval Warfare Systems Command (00) | TS |
| Program Director, Command, Control and Communications Systems Program Directorate (PD-17) | S |
| Program Director, Intelligence, Surveillance and Reconnaissance Directorate (PD-18) | S |

**Office of the Chief of Naval Operations**

| | |
|---|---|
| Chief of Naval Operations (N00) | TS |
| Executive Assistant to the Chief of Naval Operations (N00A) | S |
| Executive Director, CNO Executive Panel/Navy Long-Range Planner (N00K) | S |
| Deputy Chief of Naval Operations (Manpower/Personnel) (N1)/ Chief of Naval Personnel (PERS 00) | TS |
| Assistant Deputy Chief of Naval Operations (Manpower/Personnel) (N1B)/Deputy Chief of Naval Personnel (PERS 00B) | TS |
| Director of Naval Intelligence (N2) | TS |
| Assistant Director of Naval Intelligence for Interagency Coordination (N2K) | S |
| Director, Requirements, Plans, Policy and Programs Division (N20) | S |

| | |
|---|---|
| Director, Operational Support Division (N23) | S |
| Director, Special Projects Division (N24) | TS |
| Chief of Staff, Office of Naval Intelligence, Suitland, MD (ONI-OC) | TS |
| Deputy Chief of Naval Operations (Plans, Policy, and Operations) (N3/N5) | TS |
| Director, Strategy and Policy Division (N51) | TS |
| Director, Operations, Plans, Political Military Affairs (N31/N52) | TS |
| Deputy Chief of Naval Operations (Logistics) (N4) | TS |
| Director, Strategic Sealift Division (N42) | S |
| Director, Space, Information Warfare, Command and Control (N6) | TS |
| Executive Assistant to Director, Space, Information Warfare, Command and Control (N6A) | S |
| Deputy Director, Space, Information Warfare, Command and Control (N6B) | TS |
| Director, Fleet & Allied Requirements Division (N60) | TS |
| Deputy Chief of Naval Operations (Resources, Warfare Requirements, and Assessments) (N8) | TS |
| Director, Programming Division (N80) | TS |
| Director, Assessments Division (N81) | TS |
| Director, Fiscal Management Division (N82) | S |
| Director, Expeditionary Warfare Division (N85) | TS |
| Head, Special Warfare Branch (N851) | S |

| | |
|---|---|
| Director, Surface Warfare Division (N86) | TS |
| Head, Surface Warfare, Plans/Programs/ Requirements Assessments Branch (N861) | S |
| Head, Theater Air Defense (N865) | S |
| Director, Submarine Warfare Division (N87) | TS |
| Head, SSBN & Maintenance Branch (N871) | S |
| Head, Attack Submarine Branch (N872) | S |
| Head, Deep Submergence Branch (N873) | S |
| Head, Undersea Surveillance Branch (N874) | S |
| Head, Undersea Manpower & Training Branch (N879) | S |
| Director, Air Warfare Division (N88) | TS |
| Head, Aviation Plans/Requirements Branch (N880) | S |
| Head, Carrier & Air Station Programs Branch (N885) | S |

<u>Naval Nuclear Propulsion Program</u>

| | |
|---|---|
| Director, Naval Nuclear Propulsion Program (N00N)/ Deputy Commander, Nuclear Propulsion Directorate, Naval Sea Systems Command (SEA-08) | TS |
| Deputy Director, Naval Nuclear Propulsion Program (N00NB)/Deputy Director, Nuclear Propulsion Directorate, Naval Sea Systems Command (SEA-08) | S |
| Associate Director for Regulatory Affairs (N00NU) | S |
| Director, Nuclear Technology Division (N00NI) | S |
| Program Manager for Commissioned Submarines (N00NO) | S |
| Director, Reactor Engineering Division (N00NI) | S |
| Director, Submarine Systems Division (N00NE) | S |

**Oceanographer of the Navy**

| | |
|---|---|
| Oceanographer of the Navy (N096) | TS |

**Military Sealift Command**

| | |
|---|---|
| Commander, Military Sealift Command (N00) | TS |

**Naval Computer and Telecommunications Command**

| | |
|---|---|
| Commander, Naval Computer and Telecommunications Command (N00) | TS |

**Naval Security Group**

| | |
|---|---|
| Commander, Naval Security Group Command | TS |

**Strategic Systems Programs**

| | |
|---|---|
| Director, Strategic Systems Programs (00) | TS |

**Naval Space Command**

| | |
|---|---|
| Commander, Naval Space Command | TS |

**Navy International Programs Office**

| | |
|---|---|
| Director, Navy International Programs Office (00) | S |

**Naval Meteorology and Oceanography Command**

| | |
|---|---|
| Commander, Naval Oceanography Command | TS |

**Mine Warfare Command**

| | |
|---|---|
| Commander, Mine Warfare Command | TS |

**Naval War College**

| | |
|---|---|
| President, Naval War College | TS |

## U.S. NAVY FLEET COMMANDS

### U.S. ATLANTIC FLEET

| | |
|---|---|
| Commander in Chief, U.S. Atlantic Fleet (N00) | TS |
| Deputy and Chief of Staff, U.S. Atlantic Fleet (N01) | TS |
| Commander, Southern U.S. Atlantic Fleet (N2) | TS |
| Director of Operations, U.S. Atlantic Fleet (N3) | S |
| Director of Plans and Policy, U.S. Atlantic Fleet (N5) | S |
| Commander, Training Command, U.S. Atlantic Fleet (N002) | S |
| Commander, Naval Surface Force, U.S. Atlantic Fleet (N002A) | TS |
| Commander, Submarine Force, U.S. Atlantic Fleet | TS |
| Commander, Second Fleet (N002A) | TS |

### U.S. PACIFIC FLEET

| | |
|---|---|
| Commander in Chief, U.S. Pacific Fleet (N00) | TS |

### U.S. NAVAL FORCES EUROPE

| | |
|---|---|
| Commander in Chief, U.S. Naval Forces Europe (N014) | TS |
| Deputy Commander in Chief, U.S. Naval Forces Europe (N014) | TS |
| Chief of Staff, U.S. Naval Forces Europe (01) | S |
| Deputy Chief of Staff for Intelligence, U.S. Naval Forces Europe (N2) | S |
| Deputy Chief of Staff, Operations, U.S. Naval Forces Europe (N3) | S |
| Deputy Chief of Staff, Supply/Logistics, Europe (N4) | S |

| | |
|---|---|
| Deputy Chief of Staff, Plans, Policy, and Requirements, Europe (N5) | S |
| Deputy Chief of Staff, Command, Control, Communications and Computers, Europe (N6) | S |
| Deputy Chief of Staff, Cryptology, Europe (N8) | S |

U.S. SIXTH FLEET

| | |
|---|---|
| Commander, U.S. Sixth Fleet (00) | TS |
| Commander, Fleet Air Mediterranean/U.S. Sixth Fleet (N1) | TS |

U.S. NAVAL FORCES CENTRAL COMMAND

| | |
|---|---|
| Commander, Service Forces, U.S. Naval Forces Central Command (00) | TS |

U.S. MARINE CORPS

| | |
|---|---|
| Commandant of the Marine Corps | TS |
| Military Secretary to the Commandant of the Marine Corps | S |
| Assistant Commandant of the Marine Corps | TS |
| Director, Marine Corps Staff, Secretary of the General Staff | S |
| Deputy Chief of Staff for Plans, Policies and Operations, Marine Corps | TS |
| Deputy Chief of Staff for Aviation, Marine Corps | TS |
| Assistant Chief of Staff for Command, Control, Communications, Computers, and Intelligence (C4I)/Directorate Intelligence/Marine Corps | TS |
| Deputy Director, Intelligence Division (CI), Marine Corps | S |

**U.S. Marine Corps Combat Development Command**

| | |
|---|---|
| Commanding General, Marine Corps Combat Development Command, Quantico, VA | TS |

**U.S. Marine Corps Systems Command**

| | |
|---|---|
| Commander, Marine Corps Systems Command, Quantico, VA | TS |

**U.S. Marine Corps Forces, Atlantic/Europe**

| | |
|---|---|
| Commanding General, U.S. Marine Corps Forces, Atlantic/ Commanding General, II Marine Expeditionary Force/Commanding General, Fleet Marine Force, Europe | TS |
| Chief of Staff, Fleet Marine Corps Force, Europe | S |
| Commanding General, 2nd Marine Division, FMF, Camp LeJeune, NC (Code 6) | S |

**U.S. Marine Corps Logistics Base**

| | |
|---|---|
| Commanding General, Marine Corps Logistics Base, Albany, GA (Code 100) | S |

**U.S. Marine Corps Forces, Pacific**

| | |
|---|---|
| Commander, U.S. Marine Corps Forces, Pacific | TS |

**U.S. Marine Corps Expeditionary Forces**

| | |
|---|---|
| Commanding General, 1st Marine Division/CG, I Marine Expeditionary Force | S |
| Commanding Officer, 11th Marine Expeditionary Unit, Camp Pendleton, CA | S |
| Commanding Officer, 15th Marine Expeditionary Unit, Camp Pendleton, CA | S |
| Commanding General, 3rd Marine Division/CG, III Expeditionary Force | S |

U.S. Marine Corps Base

| | |
|---|---|
| Commanding General, Marine Corps Base, Camp Pendleton, CA | S |

U.S. Marine Corps Air Station

| | |
|---|---|
| Commanding General, Marine Corps Air Station, El Toro, (Santa Ana), CA | S |

U.S. Marine 4th Aircraft Wing

| | |
|---|---|
| Commanding General, 4th Marine Aircraft Wing, New Orleans, LA (Code 6) | S |

# CHAPTER 5

# SECURITY CLASSIFICATION GUIDES

## 5-1 BASIC POLICY

1. Security Classification Guides (SCGs) serve both legal and management functions by recording DON original classification determinations made under reference (a) and its predecessor orders. SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements.

2. The DON OCAs listed in **exhibit 4A** are required to prepare a SCG for each DON system, plan, program, or project under their cognizance which creates classified information. Updates to **exhibit 4A** can be found on the **CNO (N09N2) Homepage at www.navysecurity.navy.mil**. SCGs shall be issued as soon as practicable prior to initial funding or implementation of the relevant system, plan, program, or project. In support of this requirement, the CNO (N09N2) manages a system called the Retrieval and Analysis of Navy Classified Information (RANKIN) Program, which manages and centrally issues SCGs for the DON OCAs.

## 5-2 PREPARING SCGs

SCGs shall be prepared, in writing, in the format described in reference (b), and approved personally by an OCA who has both cognizance (i.e., program or supervisory responsibility) over the information, and who is authorized to originally classify information at the highest classification level prescribed in their SCG(s).

## 5-3 RANKIN PROGRAM

1. The primary element of the RANKIN Program is a computerized data base that provides for the standardization, centralized management and issuance of all DON SCGs. After approval by an OCA, SCGs are forwarded to the CNO (N09N2), RANKIN Program Manager, and entered into the RANKIN data base. Additionally, the RANKIN Program Manager maintains historical files for all DON SCGs.

2. Uniformly formatted SCGs are issued by the CNO (N09N) in the following major subject categories:

| | |
|---|---|
| OPNAVINST 5513.1: | DON SCGs. (Assigns specific responsibilities for guide preparation and updating) |
| OPNAVINST C5513.2: | Air Warfare Programs |
| OPNAVINST S5513.3: | Surface Warfare Programs |
| OPNAVINST S5513.4: | General Intelligence, Cover and Deception, Security and Investigative Programs |
| OPNAVINST S5513.5: | Undersea Warfare Programs |
| OPNAVINST S5513.6: | Communication and Satellite Programs |
| OPNAVINST C5513.7: | Mine Warfare Programs |
| OPNAVINST S5513.8: | Electronic Warfare Programs |
| OPNAVINST S5513.9: | Nuclear Warfare Programs |
| OPNAVINST 5513.10: | Advanced Technology and Miscellaneous Programs |
| OPNAVINST 5513.11: | Ground Combat Systems |
| OPNAVINST 5513.12: | Intelligence Research Projects |
| OPNAVINST 5513.13: | Non-Acoustic Anti-Submarine Warfare (NAASW) Programs |
| OPNAVINST 5513.14: | Space Programs |
| OPNAVINST 5513.15: | Naval Special Warfare Programs |
| OPNAVINST 5513.16: | Declassification of 25-Year Old DON Information |

Periodic updates to this category listing can be found on the CNO (N09N2) Homepage at www.navysecurity.navy.mil.

3. The OPNAVINST 5513 series contains, as enclosures, individual SCGs for systems, plans, programs, or projects related to the overall subject area of the instruction. The SCGs are automatically distributed to commands consistent with their command missions.

4. The CNO (N09N) periodically issues an index of SCGs available within the DON. Commands shall utilize the index to identify those SCGs needed to accomplish their mission. Most instructions in the OPNAVINST 5513 series are assigned National Stock Numbers (NSNs) and can be ordered through the DON supply system. Requests for instructions not assigned NSNs or requests to be placed on automatic distribution for changes and revisions to SCGs shall be addressed to the CNO (N09N2).

## 5-4 PERIODIC REVIEW OF SCGs

OCAs shall review their SCGs for accuracy and completeness at least every 5 years and advise the CNO (N09N2) of the results. Proposed changes to, and cancellations of, existing SCGs shall be sent to the CNO (N09N2) in the format described in reference (b).

## 5-5 SCGs OF MULTI-SERVICE INTEREST

SCGs for systems, plans, programs, or projects involving more than one DoD component are issued by the Office of the Secretary of Defense (OSD) or the DoD component designated by the OSD as executive or administrative agent. When designated by the OSD, commands shall report the designation to the CNO (N09N2), prepare any necessary security classification guidance, and forward it to the CNO (N09N2).

## 5-6 CONFLICT BETWEEN A SOURCE DOCUMENT AND AN SCG

In cases of apparent conflict between an SCG and a classified source document about a discrete item of information, the instructions in the SCG shall take precedence.

## REFERENCES

(a) Executive Order 12958, *Classified National Security Information*, 17 Apr 95

(b) OPNAVINST 5513.1E, *DON Security Classification Guides*, 16 Oct 95

# CHAPTER 6

# MARKING

## 6-1 BASIC POLICY

1. All classified information shall be clearly marked with the date and office of origin, the appropriate classification level and all required "associated markings" (see paragraph 6-1.5 for exceptions to this policy). "Associated markings" include those markings which identify the source of classification (or for original decisions, the authority and reason for classification); downgrading and declassification instructions; and warning notices, intelligence control markings and other miscellaneous markings (see paragraph 6-7 for guidance on the placement of associated markings).

2. The word "document" is used generically throughout this chapter not only because it describes the most common form of classified material, but to make explanations more tangible. Documents take many forms, including publications (bound or unbound), reports, studies, manuals, etc. Some types of classified material (e.g., correspondence, letters of transmittal, AIS media, recordings, photographs, and electronic messages) have special marking requirements as described in this chapter.

3. The proper marking of a classified document is the specific responsibility of the original or derivative classifier. While markings on classified documents are intended primarily to alert holders that classified information is contained in a document, they also serve to warn holders of special access, control or safeguarding requirements.

4. Documents containing "tentatively" classified information shall be marked per chapter 4, paragraph 4-14.

5. Exceptions to the basic marking policy include:

a. No classification level or associated markings shall be applied to any article or portion of an article that has appeared in the public domain (e.g., in a newspaper or magazine), even if that article is the subject of a public media compromise inquiry.

b. Documents containing RD (including CNWDI) or FRD, shall not be marked with any downgrading or declassification instructions, other than those approved by the DOE.

c. Mark classified documents provided to foreign governments, their embassies, missions, or similar official offices within the U.S., with only the highest overall classification level. Commands originating such documents shall maintain a file copy which reflects all required associated markings.

d. Classified documents shall not be marked if the markings themselves would reveal a confidential source or relationship not otherwise evident in the document.

## 6-2 DON COMMAND AND DATE OF ORIGIN

Every classified document shall indicate on the front cover, first page or title page (hereafter referred to as the "face" of the document) the identity of the DON command that originated the document (a command's letterhead satisfies this requirement) and the date the document was originated.

## 6-3 OVERALL CLASSIFICATION LEVEL MARKING

Mark (stamp, print, or permanently affix with a sticker or tape) the face and back cover, top and bottom center, of all classified documents to show the highest overall classification level of the information they contain. These markings shall be conspicuous enough (i.e. larger than the text) to alert anyone handling the document that it is classified. Include an explanatory statement on the face of any classified document which cannot be marked in this manner.

## 6-4 INTERIOR PAGE MARKINGS

1. Mark each interior page of a document (except blank pages), top and bottom center, with the highest overall classification level of any information contained on the page (see paragraph 6-7, 6-11 and 6-12 (and exhibit 6A-1) for placement of certain warning notices and intelligence control markings on interior pages). If the page is printed front and back, mark both sides of the page. Mark pages containing only unclassified information "UNCLASSIFIED."

2. An alternative interior page marking method permits each page to be marked with the highest overall classification level of information contained in the document. Using this highest overall classification scheme for interior pages, however, does not eliminate the requirement to portion mark.

## 6-5 PORTION MARKINGS

1. Mark each portion (e.g., title, section, part, paragraph or subparagraph) of a classified document to show its classification level. This requirement eliminates any doubt as to which portions of a document are classified. Place the appropriate abbreviation ("TS" (Top Secret), "S" (Secret), "C" (Confidential) or "U" (Unclassified)), immediately following the portion letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion (see **exhibit 6A-2**). The abbreviation "FOUO" may be used to designate unclassified portions containing information exempt from mandatory release to the public under reference (a) (see **exhibit 6A-3**). Additionally, place the applicable abbreviated warning notice(s) and intelligence control marking(s) (see paragraphs 6-11 and 6-12) directly after the abbreviated classification level of each portion.

2. If an exceptional situation makes individual portion markings clearly impracticable, place a statement on the face of the document describing which portions are classified, and at what classification level. This statement shall identify the classified information as specifically as would parenthetical portion markings.

3. Mark figures, tables, graphs, charts and similar illustrations appearing within a document with their classification level, including the short form(s) of any applicable warning notice(s) and intelligence control marking(s). Place these markings within, or adjacent to, the figure, table, graph or chart. Mark chart and graph captions or titles with the abbreviated classification level (including all applicable abbreviated warning notice(s) and intelligence control marking(s)). When figure or table numbers are used to identify the captions or titles, place these abbreviated marking(s) after the number and before the text (see **exhibit 6A-4**).

4. Portions of U.S. documents containing NATO or FGI shall be marked to reflect the country, international organization, and appropriate classification level (see **exhibit 6A-5**). The letter "R" shall be used for the identification of NATO RESTRICTED or Foreign Government RESTRICTED information.

5. The authority to grant waivers of the portion marking requirement rests with the Director, ISOO. Waivers granted prior to 14 October 1995 by DoD officials are no longer valid.

Requests for waivers shall be forwarded to the OASD ($C^3I$), via the CNO (N09N2), for submission to the Director, ISOO. Forward waiver requests for SAPs to the Director, Special Programs, Office of the DUSD(PS), via the CNO (N09N2), for submission to the Director, ISOO. The waiver request shall include the following:

a. Identification of the classified information or material (e.g., a certain type of document) for which the waiver is sought;

b. A detailed explanation of why compliance with the portion marking requirement is not practical;

c. An estimate of anticipated dissemination of the classified information or material; and

d. The extent to which the classified information or material may form a basis for derivative classification.

## 6-6 SUBJECTS AND TITLES

1. Mark subjects or titles with the appropriate abbreviated classification level, after the subject or title (see **exhibits 6A-2, 6A-3** and **6A-5**). When subjects or titles of classified documents are included in the reference line, enclosure line, or the body of information, the classification of the subject or title shall follow.

2. Whenever possible, subjects or titles shall be unclassified for identification and reference purposes. If a classified subject or title is unavoidable, an unclassified short title shall be added for reference purposes, for example:

"Subj: ASW OPERATIONS IN THE BATAVIAN LITTORAL ON 2 JUNE 99 (C)
(SHORT TITLE: "ASWOPS 3-99 (U))."

## 6-7 PLACEMENT OF ASSOCIATED MARKINGS

1. Associated markings are spelled out in their entirety on the face of a document. Certain associated markings, (i.e., the "Classified by," "Reason," "Derived from," "Downgrade to," "Declassify on," lines), and certain warning notices (e.g., RD, CNWDI and FRD) are placed on the face of the document in the lower left hand corner (see **exhibit 6A-1**). Other warning notices (e.g., dissemination and reproduction notices, SIOP-ESI and CRYPTO) and all intelligence control markings, are spelled out in

their entirety on the face of the document, at the bottom center of the page, above the classification level marking. See paragraph 6-23 for the proper placement of markings on correspondence and letters of transmittal.

2. Associated markings are not spelled out on interior pages. However, the short forms of certain warning notice(s), (e.g., "RESTRICTED DATA," "FORMERLY RESTRICTED DATA," "NNPI," and "CRYPTO" (see paragraph 6-11)), and the short form of all intelligence control marking(s) (see paragraph 6-12), applicable to each page, shall be marked after the classification level at the bottom center of each page. Associated markings shall not be placed on the back cover of any classified document (see exhibit 6A-1).

## 6-8 MARKING ORIGINALLY CLASSIFIED DOCUMENTS WITH THE "CLASSIFIED BY" AND "REASON" LINES

1. The "Classified by" and "Reason" lines are rarely used because an estimated 99 percent of all DON documents are derivatively classified.

2. Mark the face of a document containing originally classified information with a "Classified by" and "Reason" line (see exhibit 6A-6). The "Classified by" line shall be followed by the identity of the DON OCA (e.g., COMINEWARCOM). The "Reason" line shall indicate a concise reason for classification. These "Reason" codes may be found in reference (b).

3. Mark the face of a document containing both originally and derivatively classified information with a "Classified by" line and "Reason" line (see exhibit 6A-7). The "Classified by" line shall indicate "Multiple Sources" as the source of classification and a list of sources, as required in paragraph 6-9, shall be maintained with the file copy of the document.

## 6-9 MARKING DERIVATIVELY CLASSIFIED DOCUMENTS WITH THE "DERIVED FROM" LINE

Mark the face of a document containing only derivatively classified information with a "Derived from" line. If all of the information was derivatively classified using a single SCG or source document, identify the SCG or source document on the "Derived from" line. Include the date of the source document or SCG (unless the identification of either the source or the SCG implicitly includes the date) (see exhibit 6A-8). If more than one SCG, source document, or combination of these provide the

derivative classification guidance, place "Multiple Sources" on the "Derived from" line. However, if "Multiple Sources" is used, maintain a record of the sources on or with the file or record copy of the document. When feasible, this list should be included with all copies of the document. If the document has a bibliography, or reference list, this may be used as the list of sources, however, annotate the list to distinguish the sources of classification from other references.

**6-10 USE OF THE "DOWNGRADE TO" AND "DECLASSIFY ON" LINES**

1. When applicable, place the "Downgrade to" line on a document immediately below either the "Classified by" and "Reason" lines or the "Derived from" line. The "Downgrade to" line is used to indicate that a change in document classification level will occur on a specific date or event. The "Downgrade to" line is always used in addition to the "Declassify on" line (see **exhibits 6A-6 through 6A-8**).

2. Place the "Declassify on" line on a document immediately below the "Classified by" and "Reason" lines, or the "Derived from" line, or immediately below the "Downgrade to" line, if a "Downgrade to" line is used. The "Declassify on" line is used to indicate that a document no longer requires classification after a specific date or event, or that the document is exempt from automatic declassification (i.e., requires an "X" code) (see **exhibits 6A-3 and 6A-7**). Reference (c) discusses the use of "25X codes" as a declassification instruction applied to permanently-valuable records.

3. When derivatively classifying a document, the most restrictive downgrading and declassification instruction(s) of all the sources shall be carried forward to the newly created document.

**6-11 WARNING NOTICES**

1. Warning notices advise the holders of a document of additional protective measures such as restrictions on reproduction, dissemination or extraction. See **exhibit 8A** for a listing of distribution statements for technical documents.

2. The following warning notices are authorized for use, when applicable:

a. **Dissemination and Reproduction Notices.** Mark classified documents subject to special dissemination and reproduction

limitations, as determined by the originator, with one of the following statements on the face of the document, at the bottom center of the page, above the classification level marking:

(1) "REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR OR HIGHER DOD AUTHORITY."

(2) "FURTHER DISSEMINATION ONLY AS DIRECTED BY (insert appropriate command or official) OR HIGHER DOD AUTHORITY."

b. **RD and FRD.** Per reference (d), mark classified documents containing RD and/or FRD on the face of the document, in the lower left corner, with the applicable warning notice (the RD notice takes precedence over the FRD notice if both RD and FRD information are contained in the document) (see **exhibits 6A-9 and 6A-10**):

(1) "RESTRICTED DATA"--"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal 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."

Portion mark documents containing RD with the abbreviated form "RD" (e.g., "(TS/RD)") and portions containing FRD with the abbreviated form "FRD" (e.g., "(C/FRD)"). The short form for RD is "RESTRICTED DATA" and the short form for FRD is "FORMERLY RESTRICTED DATA." Place these short forms on interior pages, after the classification level at the bottom of each applicable page. Additionally, place these short forms after the classification level at the top left corner on the first page of correspondence and letters of transmittal.

c. **CNWDI.** CNWDI (a subset of RD) is subject to special dissemination controls. In addition to the RD notice, mark the face of a document containing CNWDI in the lower left corner with the following warning notice:

"CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION, DOD DIRECTIVE 5210.2 APPLIES"

Portion mark RD documents containing CNWDI with the abbreviated form "(N)" (e.g., "(S/RD)(N)"). Mark interior pages containing

CNWDI with the short form "CNWDI" after the classification level at the bottom center of each applicable page (see exhibit 6A-10). Place "CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION" after the classification level at the top left corner on the first page of correspondence and letters of transmittal. The marking policies and dissemination procedures for CNWDI are contained in reference (e).

d. NNPI

(1) Per reference (f), in light of the national policy prohibiting foreign disclosure of NNPI, special distribution control markings are used on correspondence and documents containing classified or unclassified NNPI. Requirements for the proper use and placement of these markings is set forth in references (f) and (g) (these markings shall only be used on NNPI documents (except for the use of "NOFORN" as the short form of an intelligence control marking (see paragraph 6-12)):

(a) "NOFORN" - NOT RELEASABLE TO FOREIGN NATIONALS;

(b) "SPECIAL HANDLING REQUIRED" - NOT RELEASABLE TO FOREIGN NATIONALS;

(c) "THIS DOCUMENT (or material) IS SUBJECT TO SPECIAL EXPORT CONTROLS AND EACH TRANSMITTAL TO FOREIGN GOVERNMENTS OR FOREIGN NATIONALS MAY BE MADE ONLY WITH PRIOR APPROVAL OF THE COMNAVSEASYSCOM"

(2) The paragraph 6-5 requirement for portion marking is waived for documents containing classified NNPI (except for NNPI classified as RD). However, in the case of a document containing both classified NNPI and non-NNPI classified information, the non-NNPI classified portions shall be portion marked as required in paragraph 6-5.

(3) Mark the following associated marking on the face of a classified NNPI document (except an NNPI document also classified as RD):

"Derived from: DOE-DoD Classification Guide,
CG-RN-1, Revision ____ dated ____
Declassify on: X2, X3, X6, X8
This document shall not be used as a basis for derivative classification guidance."

(4) Classified NNPI containing RD or FRD information is governed by the provisions of paragraphs 6-4 and 6-10. Classified NNPI not containing RD or FRD information shall include the associated markings set forth in reference (f).

(5) DOE Unclassified Controlled Nuclear Information (DOE UCNI). Mark unclassified NNPI which is also DOE UCNI per reference (f).

e. **SIOP.** Per reference (h), SIOP documents shall be marked in the same manner as any other classified document. SIOP documents released to NATO shall be marked per reference (h).

f. **SIOP-ESI.** Per reference (h), SIOP-ESI documents are subject to special dissemination controls. Mark the front and back cover of SIOP-ESI documents, center top and bottom, below the classification level marking, with the indicator "SIOP-ESI Category XX". Additionally, mark the face of SIOP-ESI documents, bottom left, with the following warning notice:

> "This (correspondence, memorandum, report, etc.) contains SIOP-ESI Category XX data. Access lists govern internal distribution."

Messages containing SIOP-ESI shall include the designator "SPECAT" and the indicator "SIOP-ESI Category XX" with the category number spelled out (e.g., SPECAT SIOP-ESI CATEGORY ONE) at the beginning of the message text immediately following the overall message classification.

g. **COMSEC**

(1) Per reference (i), the designator "CRYPTO" identifies all COMSEC documents and keying material which is used to protect or authenticate classified or sensitive unclassified government or government-derived information. The marking "CRYPTO" is not a security classification.

(2) Mark COMSEC documents and material likely to be released to contractors with the following warning notice on the face of the document, at the bottom center of the page, above the classification level marking:

> "COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance."

3. Notices for Controlled Unclassified Information are as follows:

a. **FOUO.** Per reference (a), mark the bottom face and interior pages of documents containing FOUO information with "FOR OFFICIAL USE ONLY." Classified documents containing FOUO do not require any markings on the face of the document, however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY." Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion (see **exhibit 6A-3**). Unclassified letters of transmittal with FOUO enclosures or attachments shall be marked at the top left corner with "FOR OFFICIAL USE ONLY ATTACHMENT." Additionally, mark FOUO documents transmitted outside the DoD with the following notice:

> "This document contains information exempt from mandatory disclosure under the FOIA. Exemption(s) _____ apply."

b. **DoD Unclassified Controlled Nuclear Information (DoD UCNI).**

(1) **Unclassified documents containing DoD UCNI.** Per reference (j), mark the bottom face and the back cover of unclassified documents containing DoD UCNI with "DoD Unclassified Controlled Nuclear Information." Portion mark DoD UCNI unclassified documents with the abbreviated form "(DoD UCNI)" immediately before the beginning of the portion. Mark correspondence and letters of transmittal at the top left corner on the face of the document with "DoD Unclassified Controlled Nuclear Information."

(2) **Classified documents containing DoD UCNI.** Per reference (j), mark classified documents containing DoD UCNI as any other classified document except that interior pages with no classified information shall be marked "DoD Unclassified Controlled Nuclear Information" at the top and bottom center. Portion mark classified documents that contain DoD UCNI with the abbreviated form "(DoD UCNI)" immediately before the beginning of the portion and in addition to the classification marking (e.g., "(S/DoD UCNI)"). Mark correspondence and letters of transmittal at the top left corner on the face of the document with "DoD Unclassified Controlled Information."

(3) Additionally, mark the face of documents containing DoD UCNI which are transmitted outside the DoD in the lower left corner with the following notice:

"DEPARTMENT OF DEFENSE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, EXEMPT FROM MANDATORY DISCLOSURE (5 U.S.C. 552(b)(3), as authorized by 10 U.S.C. 128)"

c. **Drug Enforcement Administration (DEA) Sensitive Information.**

(1) **Unclassified documents containing DEA Sensitive Information.** Mark the top and bottom face and back cover of unclassified documents containing DEA Sensitive information with "DEA Sensitive." Portion mark unclassified DEA Sensitive documents with the abbreviated form "(DEA)" immediately before the beginning of the portion. Mark interior pages of unclassified DEA Sensitive documents top and bottom center with "DEA Sensitive."

(2) **Classified documents containing DEA Sensitive Information.** Mark classified documents containing DEA Sensitive information as any other classified document except that interior pages with no classified information shall be marked "DEA Sensitive" at the top and bottom center. Portion mark classified documents that contain DEA Sensitive information with the abbreviated form "(DEA)" immediately before the beginning of the portion and in addition to the classification marking (e.g., "(S/DEA)").

d. **Department of State (DOS) Sensitive But Unclassified (SBU) Information.** The DOS does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. Mark DON documents containing SBU information in the same manner as if the information were FOUO.

e. **NATO and Foreign Government RESTRICTED Information.** Mark documents containing NATO and Foreign Government RESTRICTED information per paragraph 6-15.

**6-12 INTELLIGENCE CONTROL MARKINGS**

1. The policy for marking intelligence information is contained in reference (k). Mark classified documents containing intelligence information with all applicable intelligence control markings on the face of the document, at the bottom center of the

page, above the classification level. Mark interior pages containing intelligence information with the short forms of all applicable intelligence control markings after the classification level at the bottom of each applicable page. Mark portions of intelligence documents with the abbreviated form of all applicable intelligence control markings. Additionally, place the applicable intelligence control marking(s), in its entirety, after the classification level at the top left corner on the first page of correspondence and letters of transmittal (see **exhibit 6A-11**).

2. Authorized intelligence control markings are as follows:

a. "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" ("ORCON" or "OC").

(1) This marking is the most restrictive intelligence control marking and shall only be used on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. It is used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination. This control marking shall not be used when access to the intelligence information will reasonably be protected by its security classification level marking, use of any other control markings specified in reference (k), or in other DCIDs.

(2) This information shall not be used in taking investigative action without the advance permission of the originator. The short form of this marking is "ORCON"; the abbreviated form is "OC".

b. "CAUTION-PROPRIETARY INFORMATION INVOLVED" ("PROPIN" or "PR").

Use this marking with, or without, a security classification level marking, to identify information provided by a commercial firm or private source under an expressed or implied understanding that the information shall be protected as a trade secret or proprietary data believed to have actual or potential value. This marking may be used on U.S. Government proprietary data only when the U.S. Government proprietary information can provide a contractor(s) an unfair advantage such as U.S.

Government budget or financial information. The short form of this marking is "PROPIN"; the abbreviated form is "PR".

c. "NOT RELEASABLE TO FOREIGN NATIONALS" ("NOFORN" or "NF").

Use this marking to identify intelligence which, per reference (l), the originator has determined may not be disclosed or released, in any form, to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. This marking is not authorized for use in conjunction with the "AUTHORIZED FOR RELEASE TO" ("REL") marking. The short form of this marking is "NOFORN"; the abbreviated form is "NF."

d. "AUTHORIZED FOR RELEASE TO...(name of country(ies) or international organization(s))" ("REL" or "REL TO").

Use this marking when a limited exception to the marking requirements of "NOFORN" may be authorized to release the information beyond U.S. recipients. This marking is only authorized when the originator has an intelligence sharing agreement or relationship with a foreign government approved in accordance with DCI policies and procedures that permits the release of the specific intelligence information to that foreign government, but to no other in any form without originator consent. This marking is not authorized for use in conjunction with the marking "NOT RELEASABLE TO FOREIGN NATIONALS" ("NOFORN"). The abbreviated form for this marking is "REL or "REL TO (abbreviated name of country(ies) or international organizations)."

4. The obsolete intelligence control markings, "WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED" ("WNINTEL") and "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS" ("NOCONTRACT") are no longer authorized for use. While the remarking of documents bearing the obsolete intelligence control markings "WNINTEL" and "NOCONTRACT" is not required, holders of documents bearing these markings may line through or otherwise remove the markings from documents. See reference (k) for assistance in recognizing and identifying other obsolete intelligence control markings.

## 6-13 MARKING DOCUMENTS CLASSIFIED UNDER THE PATENT SECRECY ACT

1. Mark patent applications that contain official information and warrant classification per this chapter.

2. If the patent application does not contain official information that warrants classification, the procedures are as follows:

a. Place a cover sheet (or letter of transmittal) on the application with the following language:

"THE ATTACHED MATERIAL CONTAINS INFORMATION ON WHICH THE U.S. PATENT OFFICE HAS ISSUED SECRECY ORDERS AFTER DETERMINING THAT DISCLOSURE WOULD BE DETRIMENTAL TO NATIONAL SECURITY (PATENT SECRECY ACT OF 1952, U.S.C. 181-188). IT IS PROHIBITED BY LAW TO TRANSMIT OR REVEAL IN ANY MANNER SUCH INFORMATION TO AN UNAUTHORIZED PERSON. HANDLE AS THOUGH CLASSIFIED (insert the classification that would be assigned had the patent application been official information)."

b. The information shall not be released to the public; dissemination within the DON shall be controlled; the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified information.

3. If a filing of a patent application with a foreign government is approved under provisions of reference (m) and arrangements on interchange of patent information have been accomplished for defense purposes, mark the copies of the patent application prepared for foreign registration (but only those copies) at the bottom of each page as follows:

"WITHHELD UNDER THE PATENT SECRECY ACT OF 1952 (35 U.S.C. 181-188) HANDLE AS (insert classification level determined)."

## 6-14 INDEPENDENT RESEARCH AND DEVELOPMENT (IR&D)

1. IR&D may be U.S. Government sponsored, or a purely private, unsponsored effort. In either case, the product of IR&D shall not be classified unless it incorporates classified information to which the developer was given prior access.

a. If no prior access was given, classification is permissible only if the U.S. Government first acquires a proprietary interest in the information.

b. If the person or company conducting the IR&D believes that protection may be warranted in the interest of national security, they shall safeguard the information and submit it to

the cognizant DON command for security evaluation. The receiving command shall make or obtain a classification determination as if it were U.S. Government information. If negative, the originator shall be notified that the information is unclassified. If affirmative, the command shall determine if an official proprietary interest in the IR&D will be acquired. Assign proper classification if an interest is acquired. If not, the originator shall be informed that there is no basis for classification and the "tentative" classification shall be cancelled.

2. In other instances, such as an unsolicited bid, in which a firm, organization or individual submits private information to the DON for classification evaluation, follow the "tentative" classification steps specified in chapter 4, paragraph 4-14.

**6-15 MARKING DOCUMENTS CONTAINING NATO OR FGI**

1. Documents classified by a foreign government or international organization retain their original foreign classification designation or are assigned the U.S. classification equivalent listed in **exhibit 6C**, in addition to that provided by the originator, to ensure adequate protection. Authority to assign the U.S. designation does not require original classification authority.

2. When NATO or other foreign government RESTRICTED information is included in an otherwise unclassified DON document, mark the face of the document with the following statement: "This document contains NATO RESTRICTED information not marked for declassification (date of source) and shall be safeguarded in accordance with USSAN 1-69." Additionally, mark the top and bottom of each applicable page with the following statement: "This page contains (indicate NATO or country of origin) RESTRICTED information" and mark the portions accordingly (e.g., "N/R" or "UK/R").

3. Mark documents that incorporate or contain extracts of NATO classified information on the cover or first page with "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION." Mark portions to identify the NATO information and classification level (e.g., "(N/S)" or "(N/C)").

4. An FGI document marked with a classification designation which equates to RESTRICTED or an unclassified FGI document provided to a DON command on the condition that it will be treated "in confidence," shall be marked "CONFIDENTIAL - MODIFIED

HANDLING" with the identity of the originating government and whether the documents are RESTRICTED or provided "in confidence."

5. When FGI is contained in a document, mark the face of the document with the following statement: "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION," or if the identity of the foreign government must be concealed, "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION." Interior pages of documents containing FGI require no additional markings, however, mark portions to indicate the country and classification level (e.g., "(UK/C)" or "(GE/S)"). The "Derived from" line shall identify the U.S. and foreign sources. The "Declassify on" line shall contain the notation "ORIGINATING AGENCY DETERMINATION REQUIRED" or "OADR" when the identity of the foreign government must be concealed. The identity of the concealed foreign government shall be maintained with the record copy and properly protected.

6. A date or event for automatic or systematic declassification shall not be assigned to FGI unless specified, or agreed to, by the foreign entity. Protect FGI classified by the DON, under this or previous regulations, for an indefinite period. Classified records containing FGI, transferred for storage or archival purposes to the NARA or other locations, shall have accompanying documentation identifying the boxes containing such information.

## 6-16 TRANSLATIONS

Translations of U.S. classified information into a foreign language shall be marked with the appropriate U.S. classification markings and the foreign language equivalent (see **exhibit 6C**). The translation shall also clearly show the U.S. as the country of origin.

## 6-17 NICKNAMES, EXERCISE TERMS AND CODE WORDS

1. Reference (n) governs the assignment, control, and use of nicknames, exercise terms and code words. Mark them as follows:

a. Nicknames are a combination of two unclassified words with an unclassified meaning (e.g., "MUD ROOM (U)").

b. An exercise term is a combination of two non-code words which may or may not be classified and may or may not have a classified meaning (e.g., "POTATO HEAD (U)" or "DUD SPUD (C)").

c. A code word is a single classified word with a classified meaning (e.g., "BRIEFCASE (C)" or "RETIREMENT (S)").

## 6-18 CLASSIFICATION BY COMPILATION

1. When individual items of unclassified or classified information are combined, classification or higher classification by compilation may result. Classification by compilation is based on an existing SCG or an original decision by an approved OCA.

2. Place a statement on the face of a document classified by compilation which explains the reason(s) for the higher classification level. Include in your statement:

a. The fact that the individual parts are unclassified or are of a lower classification;

b. The reason why the compilation warrants classification or a higher classification; and

c. The authority for the compilation classification.

An example of a compilation statement is as follows: "Individual portions of this document reveal various unclassified operational frequencies of the AN/SPG-149 radar. However, the compilation of those frequencies reveals the overall frequency band of the AN/SPG-149 radar. Per OPNAVINST S5513.8, enclosure (103), the frequency band of the AN/SPG-149 is classified Confidential-X3."

3. If portions, standing alone, are unclassified, but the compilation of the unclassified portions make the document classified, mark each portion as unclassified but mark the face of the document and interior pages with the classification level of the compilation. This principle also applies if the individual portions are classified at one level, but the compilation is of a higher classification level.

## 6-19 CHANGES TO EXISTING CLASSIFIED DOCUMENTS

1. If a change is being issued to an existing classified document, the originator of the change shall ensure that the changed pages are properly marked and consistent with the overall marking style of the basic document.

2. If a document has a front cover designed for permanent use and is frequently revised, place a statement on the lower left corner of the cover which states, "SEE TITLE (or first) PAGE FOR CLASSIFICATION AUTHORITY AND DECLASSIFICATION INSTRUCTIONS." The title or first page can then be changed as necessary.

3. In a change transmittal, a pen change for the front cover, title page, or first page may be included. If a change consists of interior pages only, the text of the change transmittal shall include the statement, "THE DECLASSIFICATION INSTRUCTIONS ASSIGNED TO THE BASIC DOCUMENT APPLY."

**6-20 MARKING TRAINING OR TEST DOCUMENTS**

1. Mark an unclassified training document which is classified for training purposes only to show that it is actually unclassified. Place a statement on each applicable page of the training document as follows: "THIS PAGE IS UNCLASSIFIED BUT MARKED AS (insert classification) FOR TRAINING PURPOSES ONLY."

2. Mark all applicable pages of an unclassified test document which will become classified when filled in as follows: "THIS (document, page, test, etc.) IS UNCLASSIFIED BUT (insert classification) WHEN FILLED IN." This policy can be applied to any unclassified document (e.g., logs and worksheets) which will later become classified when filled in.

**6-21 MARKING CLASSIFIED DOCUMENTS WITH COMPONENT PARTS**

If a classified document has components likely to be removed and used or maintained separately, mark each component as a separate document. Examples are annexes or appendices to plans, major parts of a report, sets of reference charts and AIS printout portions (see paragraph 6-32). If the entire major component is unclassified, mark it as "UNCLASSIFIED," on its face, top and bottom center, and add a statement "ALL PORTIONS OF THIS (annex, appendix, etc.) ARE UNCLASSIFIED." No further markings are required on such a component.

**6-22 REMARKING UPGRADED, DOWNGRADED OR DECLASSIFIED DOCUMENTS**

1. Upon notification, holders of classified documents that have been upgraded, downgraded or declassified, shall immediately remark the affected portions. Place on the face of the document the authority for the change, the date of the action, and the identity of the person making the change(s) (e.g., "PORTIONS DOWNGRADED TO CONFIDENTIAL PER NAVSEA LTR 09T1 SER 8S345 OF

22 JUN 99 BY MS. V. CICALA ON 29 JUN 99," or "DECLASSIFIED PER CNO MESSAGE DTG 151634Z NOV 96 ON 18 NOV 96 BY DR. ED MARSHALL, CNO (N874)").

2. When the volume of documents is such that prompt remarking of each classified item cannot be accomplished without interfering with operations, the custodian shall attach upgrading, downgrading or declassification notices to the storage unit (e.g., a container drawer, lateral file, etc.).

**6-23 CLASSIFYING FROM SOURCE DOCUMENTS WITH OLD DECLASSIFICATION INSTRUCTIONS**

1. A newly created document which derives its classification from a source document or SCG issued prior to 1 August 1982, shall be marked as follows:

a. If the source document or the SCG specifies a declassification date or event, the date or event shall be carried forward to the newly created document.

b. If the source document or the SCG gives an indeterminate declassification date or event (e.g., "OADR" or "Review on: 17 JAN 2001"), the document shall be marked "Source marked OADR, source dated (date of source)," and the OCA identified on the source document shall be consulted to determine the classification duration of the document.

**6-24 CORRESPONDENCE AND LETTERS OF TRANSMITTAL**

1. **Correspondence.** Classified correspondence is marked in the same manner as any other classified document, except the upper left corner is also marked with the highest overall classification level followed by the short forms of certain warning notices (except NNPI, which is marked per reference (f)) (see paragraph 6-11) and all applicable intelligence control markings in their entirety (see paragraph 6-12).

2. **Letters of transmittal.** A letter of transmittal may have a classified document, or documents, enclosed with or attached to it. The letter of transmittal may itself contain information classified equal to, or higher than, the classified document it is transmitting. Most often, the letter of transmittal itself is unclassified or classified at a lower level than its enclosures or attachments.

a. **Unclassified letters of transmittal.** Mark only the face of an unclassified letter of transmittal, top and bottom center, with the highest overall classification level and all applicable warning notices and intelligence control markings of its classified enclosures or attachments (the associated markings found in paragraphs 6-8 through 6-10, e.g., the "Derived from" and "Declassify on" lines among others, shall not be marked on the face of an unclassified letter of transmittal). Provide instructions, at the top left corner of the letter of transmittal, to indicate the highest overall classification level of the transmittal (including all applicable warning notices and intelligence control markings in paragraph 6-24.1 format). Additionally, indicate how the classification level of the letter of transmittal can be lowered through removal of its various enclosures or attachments. For example, if an unclassified transmittal has three enclosures, one Secret (enclosure (1)) and two Confidential (enclosures (2) and (3)), mark the transmittal "SECRET--CONFIDENTIAL UPON REMOVAL OF ENCLOSURE (1)-UNCLASSIFIED UPON REMOVAL OF ENCLOSURES (1) THROUGH (3)" (see **exhibit 6A-12**). Interior pages (if any) of unclassified letters of transmittal, which are transmitting classified enclosures or attachments, need not be marked or alternatively may be marked as "UNCLASSIFIED."

b. **Classified letters of transmittal.** Mark classified letters of transmittal in the same manner as any other classified document (see paragraph 6-1). Additionally, mark a classified letter of transmittal:

(1) Which has enclosures or attachments classified at a higher level, with the highest overall classification level and all applicable warning notices and intelligence control markings of its enclosures or attachments and the transmittal itself. Provide instructions, at the top left corner, to indicate the highest overall classification level of the transmittal (including all applicable warning notices and intelligence control markings in paragraph 6-24.1 format). Additionally, indicate how the classification level of the letter of transmittal can be lowered through removal of its various enclosures or attachments. For example, if the letter of transmittal itself is CONFIDENTIAL but has one enclosure which is SECRET, mark the transmittal, "SECRET--CONFIDENTIAL UPON REMOVAL OF ENCLOSURE (1)" (see **exhibit 6A-13**).

(2) Which is classified higher than or equal to the classification level of its enclosures or attachments, at the top left corner with the highest overall classification level and all applicable warning notices and intelligence control markings of

its enclosures or attachments and the transmittal itself. Provide instructions, at the top left corner, to indicate the highest overall classification level of the transmittal (including all applicable warning notices or intelligence control markings in paragraph 6-24.1 format). Additionally, indicate how applicable warning notices and intelligence control markings can be removed through removal of various enclosures or attachments. For example, if a letter of transmittal classified SECRET is transmitting a document classified CONFIDENTIAL/NOT RELEASABLE TO FOREIGN NATIONALS (enclosure (1)), mark the transmittal "SECRET/NOT RELEASABLE TO FOREIGN NATIONALS--SECRET UPON REMOVAL OF ENCLOSURE (1)."

3. There are no marking requirements for unclassified letters of transmittal which are transmitting only unclassified enclosures or attachments, with the exception of the controlled unclassified information specified in paragraph 6-11.3.

**6-25 MARKING ELECTRONICALLY-TRANSMITTED CLASSIFIED MESSAGES**

1. Mark classified electronically-transmitted messages in the same manner as a classified document, with the following modifications:

a. The first item of the text shall be the highest overall classification level of the message, and may be printed by an AIS, provided the marking stands out from the rest of the text. In older AISs this may be achieved by surrounding the markings with asterisks or other symbols.

b. The short forms of certain warning notices and all intelligence control markings, shall be spelled out following the message classification level which precedes the message subject line (see paragraphs 6-11 and 6-12).

c. Classified messages shall be portion marked per paragraph 6-5. However, certain preformatted messages, such as RAINFORM, CASREP and similar reporting formats, need not be portion marked as they do not contain identifiable portions. The overall classification, downgrading and declassification markings satisfy the marking requirements for these type messages.

d. The proper completion of the "DECL" line for messages is outlined in **exhibit 6B**.

## 6-26 MARKING CLASSIFIED FILES, FOLDERS AND GROUPS OF DOCUMENTS

Mark classified files, folders and similar groups of documents on the outside of the folder or holder. A classified document cover sheet (SFs 703, 704 or 705) attached to the front of the holder or folder will satisfy this requirement. These SFs need not be attached when the file or folder is in secure storage.

## 6-27 MARKING CLASSIFIED BLUEPRINTS, SCHEMATICS, MAPS AND CHARTS

Mark classified blueprints, engineering drawings, charts, maps, and similar items, not contained in classified documents, top and bottom center, with their highest overall classification level and all applicable associated markings. Mark their subjects, titles and legends as required by paragraph 6-6. If rolled or folded, clearly mark these or other large items so the highest overall classification level is clearly visible on the outside (see **exhibit 6A-14**).

## 6-28 MARKING CLASSIFIED PHOTOGRAPHS, NEGATIVES, AND UNPROCESSED FILM

1. Mark classified photographs and negatives with their highest overall classification level and all applicable associated markings. If this is not possible, place these markings on the reverse side of the photograph or negative or include accompanying documentation. Clearly show the classification level and all applicable associated markings on reproductions of photographs (see **exhibit 6A-15**).

2. Mark classified roll negatives and positives, and other film containing classified, with their highest overall classification level and all applicable associated markings. Place these markings on the canister (if one is used) and the film itself. When placed on the film itself, place the markings at the beginning and end of the roll. When self-processing film or paper is used to photograph or reproduce classified information, the negative of the last exposure shall not be allowed to remain in the camera. Remove all parts of the last exposure, secure, or destroy it as classified waste; otherwise safeguard the camera as classified.

## 6-29 MARKING CLASSIFIED SLIDES AND TRANSPARENCIES

1. Mark classified slides and transparencies with the highest overall classification level and all applicable associated markings on both the image area and the border, holder or frame.

Portion mark the information in the image area of the item (see **exhibit 6A-15**).

2. If a group of classified slides or transparencies are used together and maintained together as a set, mark only the first slide or transparency of the set with the highest overall classification level and all associated markings. Thereafter, mark each slide or transparency with the overall classification level and the short forms of all applicable warning notices and intelligence control markings. Classified slides or transparencies permanently removed from such a set shall be marked as separate documents (see **exhibit 6A-15**).

**6-30 MARKING CLASSIFIED MOTION PICTURE FILMS AND VIDEOTAPES**

Mark classified motion picture films and videotapes with the highest overall classification level and all applicable associated markings at the beginning and end of the played or projected portion. A clear audible statement announcing the highest overall classification level shall be made at the beginning and end of any motion picture film or videotape to ensure that listeners or viewers understand that classified information is being presented. Mark motion picture reels and videotape cassettes with the highest overall classification level and all applicable associated markings. Mark containers for reels and cassettes in the same manner (see **exhibit 6A-16**).

**6-31 MARKING CLASSIFIED SOUND RECORDINGS**

Classified sound recordings shall have a clear audible statement announcing the overall classification level at the beginning and end of the recording. Mark recording reels or cassettes with the highest overall classification level and all applicable associated markings. Mark containers for reels and cassettes in the same manner (see **exhibit 6A-17**).

**6-32 MARKING CLASSIFIED MICROFORMS**

1. Mark classified microfilm, microfiche, and similar media with the highest overall classification level in the image area that can be read or copied. Apply this marking so it is visible to the unaided eye. Place associated markings either on the item or included in accompanying documentation.

2. Mark protective sleeves or envelopes containing microfiche with the highest overall classification level and all applicable associated markings.

## 6-33 MARKING CLASSIFIED REMOVABLE AIS STORAGE MEDIA

1. **External Markings.** Mark removable AIS storage media with the highest overall classification level using the appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI AIS media)) and include the abbreviated form of all applicable warning notices and intelligence control markings (see paragraphs 6-11 and 6-12) of the information contain therein. (Removable AIS storage media is any device in which classified data is stored and is removable from a system by the user or operator (i.e., optical disks, CD-ROMS, removable hard drives, tape cassettes, etc.) (see **exhibit 6A-18**)).

2. **Internal Markings.** Program the software of classified AISs storing information in a readily accessible format to mark each classified file stored by the system with the highest overall classification level and all applicable associated markings (i.e., in the same manner as any other classified document). Additionally, mark the outside of AIS media storing classified files programmed in a readily accessible format with the highest overall classification level and all applicable warning notices and intelligence control markings. AIS media containing classified files not programmed in a readily accessible format shall be marked on the outside with the highest overall classification level and all applicable associated markings (normally a sticker or tag) or have marked documentation kept with the media (see **exhibit 6A-18**).

3. ISSOs shall ensure that AISs provide for classification designation of data stored in internal memory or maintained on fixed storage media.

## 6-34 MARKING CLASSIFIED DOCUMENTS PRODUCED BY AIS EQUIPMENT

1. Mark documents produced on AISs which function as word processing systems per paragraph 6-33. Special provisions for marking some AIS-generated classified documents are as follows:

a. Mark interior pages of fan-folded printouts with the highest overall classification level. These markings shall be applied by the AISs even though they may not be conspicuous from the text. Mark the face of the document with all required associated markings or place these markings on a separate sheet of paper attached to the front of the printout.

b. Mark portions of AIS printouts removed for separate use or maintenance as individual documents (see **exhibit 6A-19**).

## 6-35 MARKING MISCELLANEOUS CLASSIFIED MATERIAL

Handle materials such as, rejected copies, typewriter ribbons, carbons, and other similar items developed during the production of a classified document, in a manner that adequately protects the material. Promptly destroy such material when no longer needed. There is no need to mark this material as classified unless necessary to ensure its protection.

## REFERENCES

(a) SECNAVINST 5720.42E, *DON Freedom of Information Act (FOIA) Program*, 5 Jun 91

(b) OPNAVINST 5513.1E, *DON Security Classification Guides*, 16 Oct 95

(c) OPNAVINST 5513.16A, *Declassification of 25-Year Old DON Information*, 8 Apr 96 (NOTAL)

(d) Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act* 30 Aug 54, as amended

(e) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(f) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(g) CG-RN-1 (Rev. 3), *DOE-DoD Classification Guide for the Naval Nuclear Propulsion Program (U)*, Feb 96 (NOTAL)

(h) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(i) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(j) OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI)*, 11 Feb 93

(k) DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*, 30 Jun 98 (NOTAL)

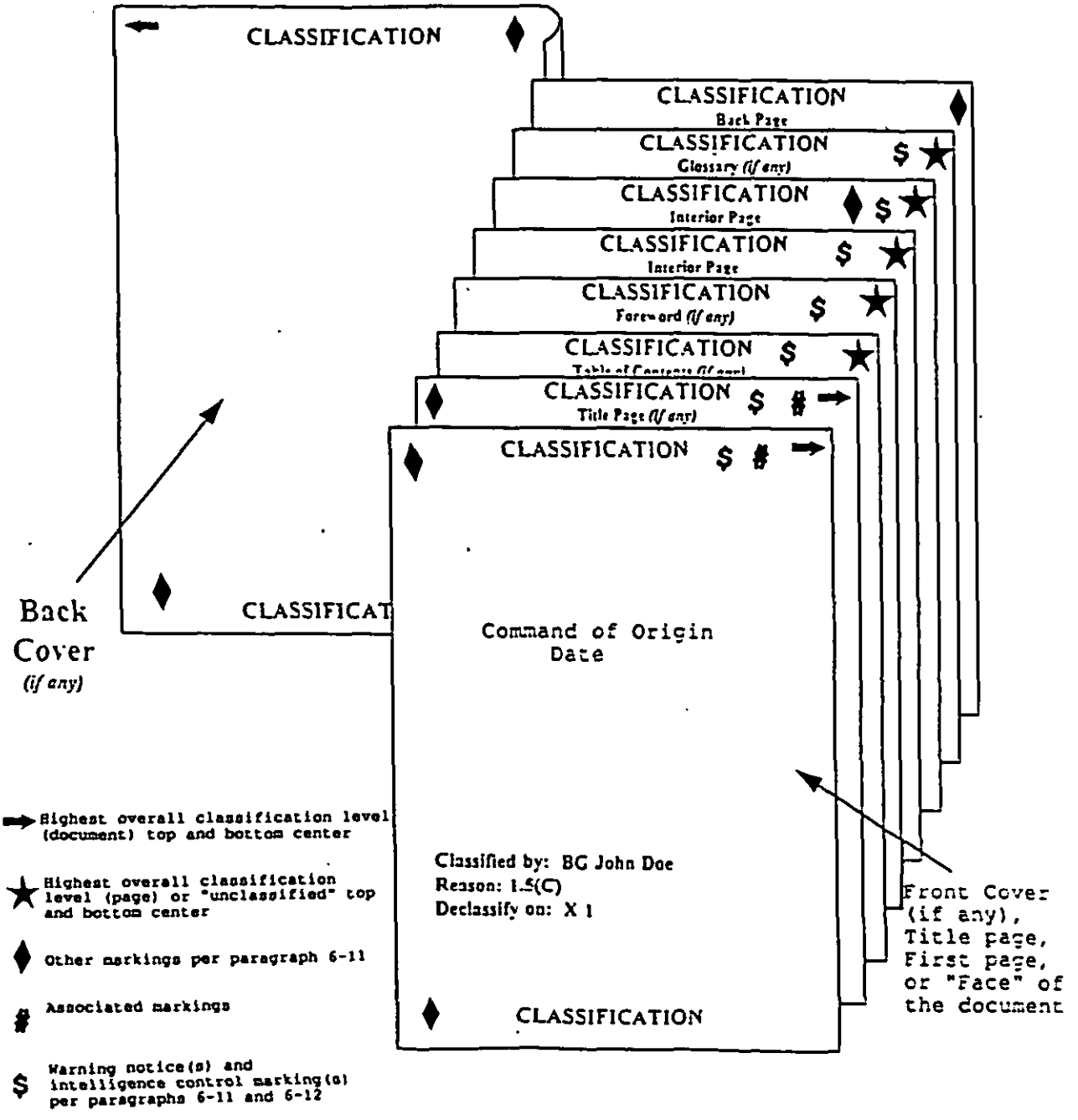
(l) DCID 5/6, *Intelligence Disclosure Policy*, 30 Jun 98 (NOTAL)

(m) Title 35, U.S.C., Section 181-188, *The Patent Secrecy Act of 1952*

(n) OPNAVINST 5511.37C, *Policy and Procedures for the use of Nicknames, Exercise Terms and Code Words*, 22 Jul 97 (NOTAL)

EXHIBIT 6A

# OVERALL AND PAGE CLASSIFICATION MARKINGS



CONFIDENTIAL

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

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

CONFIDENTIAL

MEMORANDUM

From: N09N2
To: N1

Subj: PORTION MARKINGS (U)

1. (U) Apply portion markings to every part of a classified document. The objective of portion markings is to eliminate doubt as to which portions of a classified document contain or reveal classified information.

2. (U) Mark each portion with the highest overall classification level and all warning notices and intelligence control markings applicable to the information contained in that portion. For example, this paragraph contains only "unclassified" information, therefore, it is marked with "(U)" the abbreviation for "unclassified."

a. (C) This portion, a "subparagraph" of paragraph 2, contains "Confidential" information, therefore, it is marked with "(C)" the abbreviation for "Confidential."

(1) (C) This portion, a "subparagraph" of "subparagraph" 2.a., also contains "Confidential" information, therefore, it is also marked with "(C)".

3. (C) The highest overall classification level of this document, according to its portion markings, is "Confidential," hence the document is marked as such.

S. L. POTTS
Director, Security Review

Derived from: OPNAVINST S5513.5B, enclosure (17)
Declassify on: 31 October 1998

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

CONFIDENTIAL

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

SECNAVINST 5510.36
IN REPLY REFER TO 17 MAR 1998

5510
Ser N09N2/7S123456
(Date)

SECRET

From: Chief of Naval Operations
To: Commander, Naval Space Command

Subj: MARKING CLASSIFIED INFORMATION CONTAINING FOUO INFORMATION (U)

1. (FOUO) Classified information or material containing FOUO information shall be marked per this regulation. No additional markings are required merely because it contains FOUO information.

2. (FOUO) Since FOUO information is, by definition unclassified, "FOUO" is an acceptable portion marking substitute for "U." Additionally, pages that contain only FOUO information, with no classified information, may likewise be marked "FOR OFFICIAL USE ONLY" as an acceptable substitute for "Unclassified."

3. (S) Letters of transmittal that have no classified information or material enclosed or attached to them, but have FOUO enclosures or attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

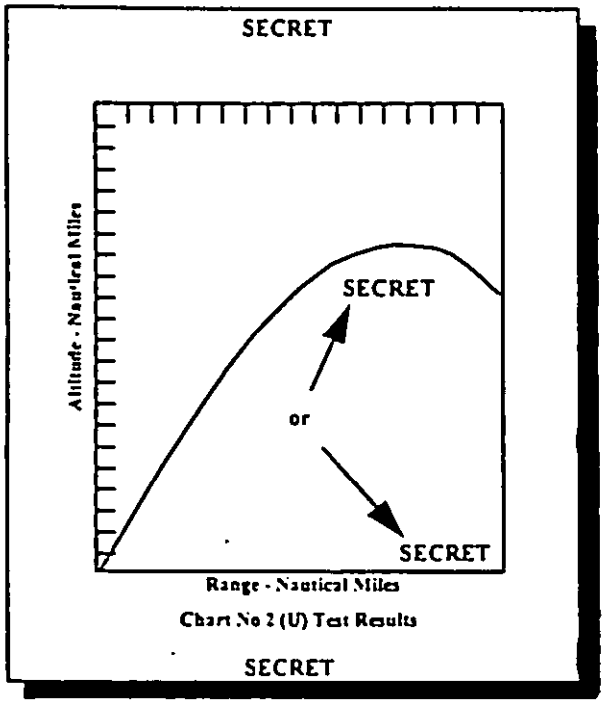
4. (FOUO) The marking "FOUO" alerts holders that the information may be withheld under exemptions (b)(2) through (b)(9) of the Freedom of Information Act (FOIA) Program, outlined in SECNAVINST 5720.42E. The marking "FOUO" may only be terminated by the originator or other competent authority, such as Initial Denial Authority (IDA) or appellate authority, when the information no longer requires protection from public disclosure. If practical, all known holders will be notified to remove this marking.

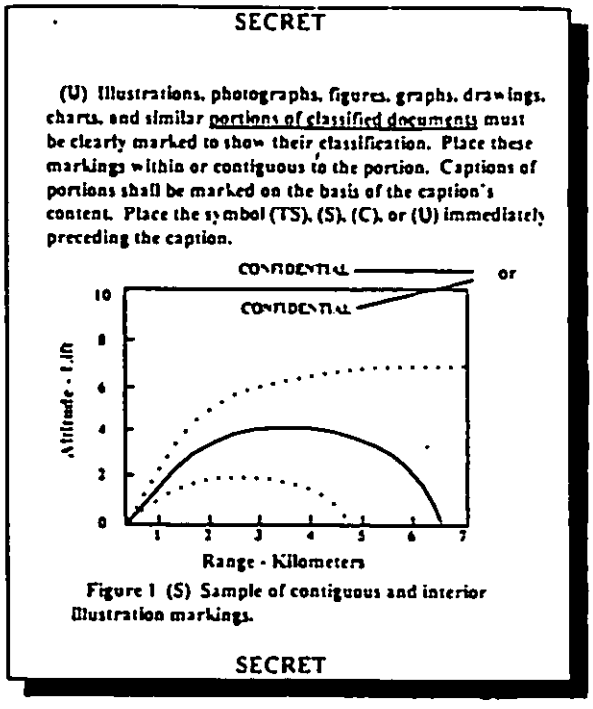
C. G. OMARA
Head, Security Branch

Derived from: OPNAVINST S5513.6C, enclosure (4)
Declassify on: X3

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

# INTERIOR PAGES WITH A CHART




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

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

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

SECNAVINST 5510.36

17 MAR 1999

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

SECRET

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

Subj: FOREIGN GOVERNMENT INFORMATION (FGI) (U)

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

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

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

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

B. S. GOLD
Special Assistant for
Security

Derived from: Multiple Sources
Declassify on: X5

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

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

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

17 MAR 1999

**SECRET**

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

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

SECRET

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

Subj: MARKING AN ORIGINALLY CLASSIFIED DOCUMENT (U)

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

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

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

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

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

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

**SECRET**

SECRET

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

SECNAVINST 5510.36
17 MAR 1999

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

SECRET

From: Chief of Naval Operations
To: Commandant of the Marine Corps

Subj: MARKING DOCUMENTS CONTAINING BOTH ORIGINAL AND DERIVATIVE CLASSIFICATION (U)

1. (S) Mark the face of documents containing original and derivative classification with "Classified by: Multiple Sources." Include a "Reason," "Downgrade to," (if applicable), "Declassify on" line, and all applicable warning notices and intelligence control markings per paragraphs 6-11 and 6-12 of this regulation.

2. (U) Maintain a listing of the derivative source(s), in addition to the identity of the OCA(s) making the original decision(s), with the file copy.

R. W. MARSH
Program Manager

Classified by: Multiple Sources
Reason: 1.5a
Declassify on: X3

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

SECRET

17 MAR 1999

**SECRET**

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

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

SECRET

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

Subj: MARKING A DERIVATIVELY CLASSIFIED DOCUMENT (U)

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

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

B. A. FITZ
Security Officer

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

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

**SECRET**

# WARNING NOTICES AND INTELLIGENCE CONTROL MARKINGS

**RESTRICTED DATA**
"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions"

**FORMERLY RESTRICTED DATA**
"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, Atomic Energy Act of 1954"

**CNWDI**
"Critical Nuclear Weapons Design Information, DoD Directive 5210.2 Applies"

**PROPIN**
"Caution Proprietary Information Involved"

**NOFORN**
"Not Releasable to Foreign Nationals"

**ORCON**
"Dissemination and Extraction of Information Controlled by Originator"

**NATO**
"This document contains NATO classified information. All users must be cleared for access to NATO information"

SECRET

Originating Command
Date

Classified by: David L. Brant
CNO (N09N)
Reason: 1.5(c)
Declassify on: X1

SECRET

Warning notices and intelligence control markings serve to notify holders that certain information requires additional protective measures (see paragraphs 6-11 and 6-12 for a complete listing and placement of these notices and markings).

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

**SECRET**

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

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

SECRET/RESTRICTED DATA/CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION

From: Chief of Naval Operations
To: Commanding Officer, Naval Research Laboratory

Subj: MARKING RD (INCLUDING CNWDI) AND FRD (U)

1. (S/RD) Portions containing Restricted Data shall have the abbreviated marking "RD."

2. (C/FRD) Portions containing Formerly Restricted Data shall have the abbreviated marking "FRD."

3. (S/RD)(N) Restricted Data portions that are also Critical Nuclear Weapons Design Information shall be marked with "N" in separate parentheses following the classification level portion marking. CNWDI is always Top Secret or Secret RD.

4. (U) Mark the face of documents containing RD (including CNWDI) and FRD with the applicable warning notice at the lower left corner. These documents shall not be marked with downgrading or declassification instructions. If a document contains both RD and FRD, overall markings will reflect only the RD marking as this marking takes precedence.

A. A. ANDERSEN
Security Manager

Derived from: CG-W-5

"RESTRICTED DATA"
"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions"

"CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION, DOD DIRECTIVE 5210.2 APPLIES"

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET/RESTRICTED DATA/CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION" FOR TRAINING PURPOSES ONLY

**SECRET**

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

SECNAVINST 5510.36

17 MAR 1999

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

SECRET/NOT RELEASABLE TO FOREIGN NATIONALS/DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR

MEMORANDUM

From: N09N2
To: N2

Subj: INTELLIGENCE CONTROL MARKINGS (U)

1. (S/NF/OC) Intelligence control markings are spelled out in their entirety on the face of the document. Mark interior pages with the short form(s) of the appropriate intelligence control marking(s) (i.e., "NOFORN" for "NOT RELEASABLE TO FOREIGN NATIONALS"; "REL TO" for "AUTHORIZED FOR RELEASE TO..." (name of country or countries); "PROPIN" for "CAUTION-PROPRIETARY INFORMATION INVOLVED"; and "ORCON" for "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR"). The intelligence short form marking follows the overall page classification level at the bottom center of each applicable interior page.

2. (S/NF) Mark paragraphs and subparagraphs with the abbreviated form(s) of the appropriate intelligence control marking(s) (i.e., respectively "NF"; "REL" (followed by the abbreviated name of the country or countries); "PR"; and "OC"). This abbreviated intelligence control marking follows the paragraph or subparagraph classification portion marking (separated with either a "/" or "-").

3. (U) Mark tables, figures, and charts in a similar manner. **The intelligence control markings "Warning Notice-Intelligence Sources or Methods Involved (WNINTEL)" and "Not Releasable to Contractors/Consultants (NOCONTRACT)" are no longer authorized for use.**

M. R. BROWNS
By direction

Derived from: OPNAVINST 5513.4D, enclosure (17)
Declassify on: X1

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

17 MAR 1999

**SECRET**

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

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

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

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

Subj: UNCLASSIFIED LETTER OF TRANSMITTAL WITH CLASSIFIED ENCLOSURES OR ATTACHMENTS

Ref: (a) Minutes of Naval Reactor Planning Group

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

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

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

V. L. CICADA
By direction

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

**SECRET**

**SECRET**

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

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

SECRET--CONFIDENTIAL upon removal of enclosure (2)

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

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

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

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

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

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

MARYANNE BATES
By direction

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

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

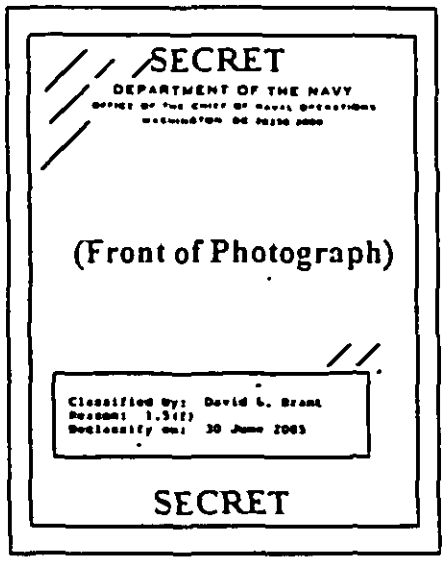
**SECRET**

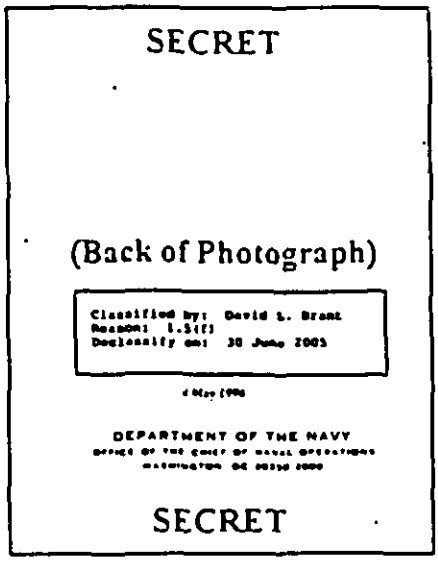
# ROLLED OR FOLDED DOCUMENTS

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

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

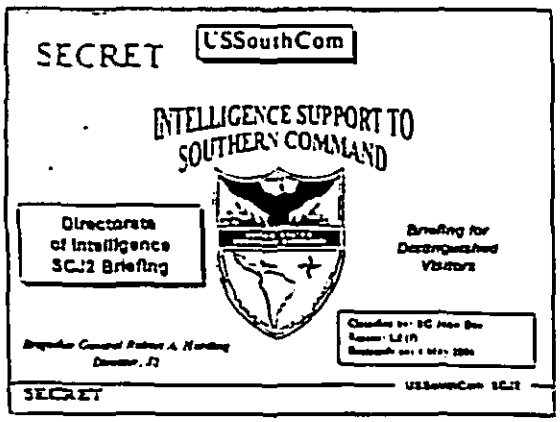
## PHOTOGRAPHS, SLIDES AND TRANSPARENCIES



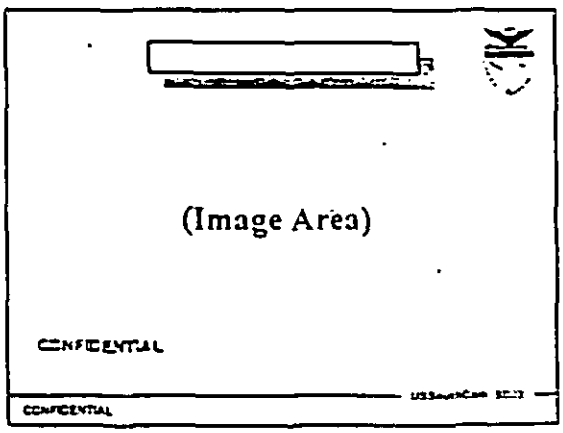




Photograph

Mark the face of a classified photograph with its highest overall classification level and associated markings, if possible. If not, place these markings on the reverse side of the photograph. These markings may be stamped or permanently affixed by pressure tape, labels or other similar means.




Cover Slide

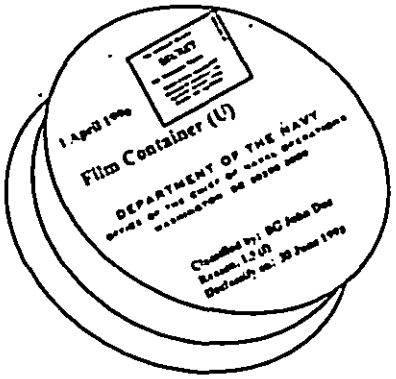


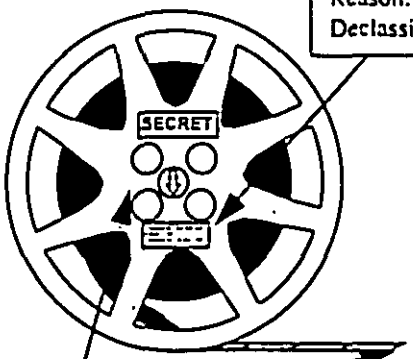

Interior Slide

Mark slides or transparencies with their highest overall classification level and associated markings on the image area, border, holder or frame. Groups of slides or transparencies used and stored together as a set shall be marked with their highest overall classification level and associated markings with the exception of the associated markings "Classified by," "Reason," "Derived from," and "Declassify on" which shall be marked on the image area of the cover slide or transparency only.

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

# MOTION PICTURE FILMS, VIDEOTAPES AND CONTAINERS

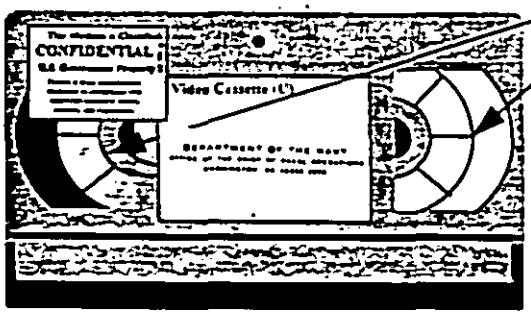



Classified By: BG John Doe
Reason: 1.5(f)
Declassify on: 30 June 1998

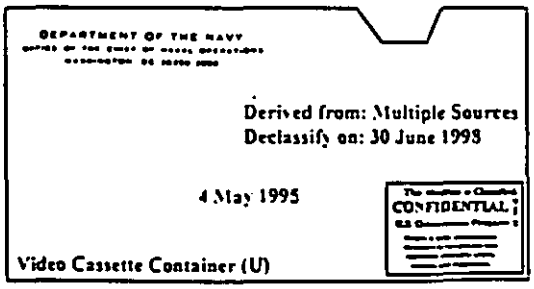
At the beginning and end of each reel

SECRET
Classified By: BG John Doe
Reason: 1.5 (f)
Declassify on: 30 June 1998




CONFIDENTIAL
Derived from: Multiple Sources
Declassify on: 30 June 1998

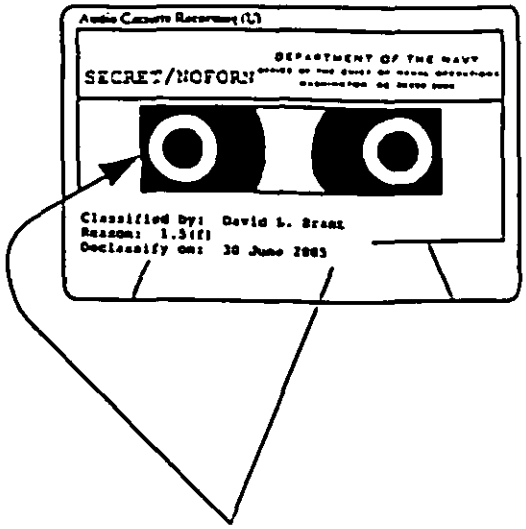
At the beginning and end of each tape.

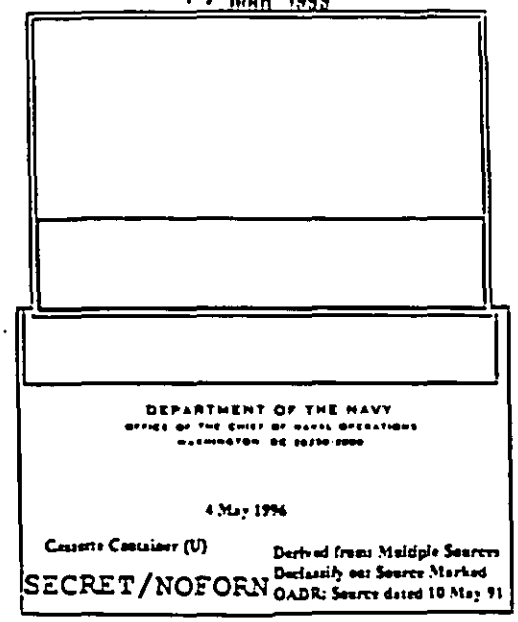



Classified motion picture films, videotapes and their titles shall be prominently marked, visible when projected, at the beginning and end of the production with the highest overall classification level and associated markings of the information they contain. Mark classified films, videotapes, and their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

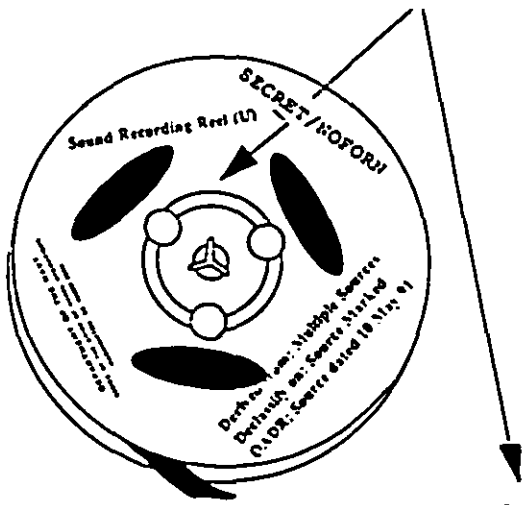
**THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" AND "CONFIDENTIAL" FOR TRAINING PURPOSES ONLY**

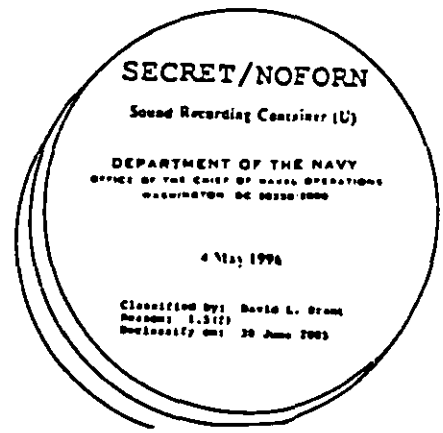
## SOUND RECORDINGS AND CONTAINERS




"The information on this recording is classified "SECRET-Not Releasable to Foreign Nationals," and is "Derived from: Multiple Sources, Declassify on: Source Marked OADR dated 10 May 91."

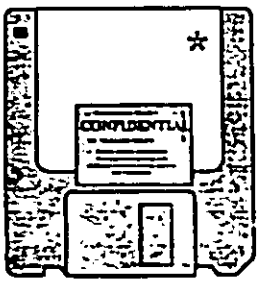


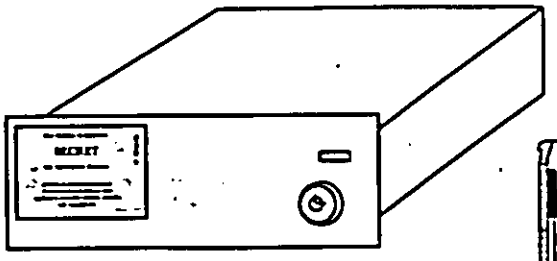

Classified sound recordings shall include an audible statement at the beginning and end of each recording identifying the highest overall classification level and associated markings of the recorded information. Containers of classified reels, cassettes, videotapes, and motion picture films shall be prominently marked with the highest overall classification level and associated markings of the information contained therein.

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

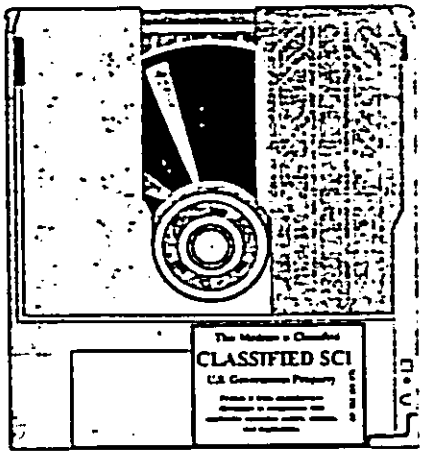
# REMOVABLE AIS MEDIA



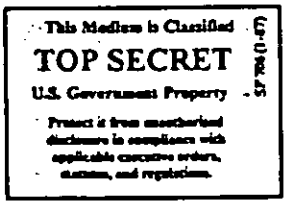

3.5" Disks

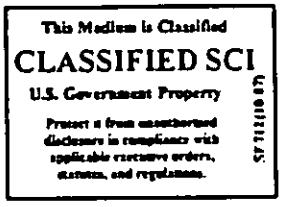


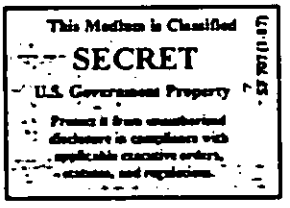
Removable Hard Drives

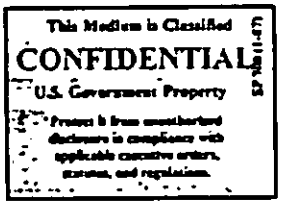


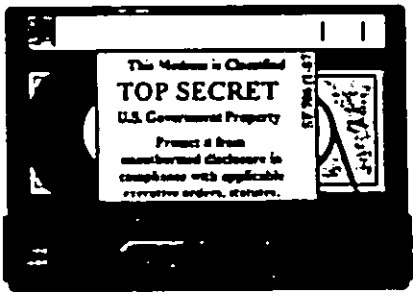

CD Backup Storage Disks



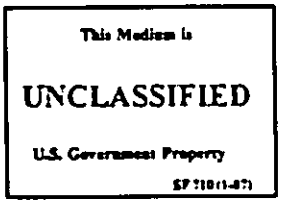



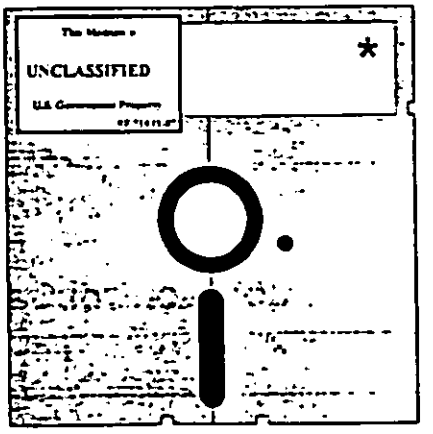




Tape Backups




5.25" Disks

Removable AIS storage media and devices used with AIS systems and word processors shall be marked using the appropriate SF label to indicate the highest overall classification level of information contained therein.

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

# PAGES OR PORTIONS REMOVED FROM AIS PRINTOUTS

CONFIDENTIAL

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

16 May 1996

(U) This portion is UNCLASSIFIED
(C) This portion is CONFIDENTIAL

Derived from: Multiple Sources
Declassify on: Source Marked OADR;
Source dated 20 Sept 1994

CONFIDENTIAL

Mark pages or portions removed from AIS printouts for separate use or maintenance as individual documents. Include the highest overall classification level and all required associated markings for all pages or portions removed.

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

## EXHIBIT 6B

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

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

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

**"DECL/"**

*Field 1* (Derivative or Original Source (abbreviate as "**DERI:**" or "**ORIG:**" respectively) for Classification (this is a mandatory field); remember that an estimated 99 percent of all DON classification decisions are derivative))"/"

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

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

*Field 4* (Declassification Exemption Code ("X" Code) (This field is conditional, i.e., the "DECL" set must contain this field or field 3, but not both) (The allowable entries for this field are

contained in Table 2))"/" (with more data to follow) or "//" (to end the set).

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

{Field 2}

TABLE 1

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

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

{Field 4}

TABLE 2

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

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

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

**EXAMPLE 1:** DECL/DERI:MULTIPLE SOURCES/-/-/X4//

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

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

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

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

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

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

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

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

**EXAMPLE 6:** DECL/DERI:C7F OPORD JASWEX 2-99/-/-/X3/-/X5//

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

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

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

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

**EXAMPLE 11:** DECL/DERI:USS KNOX LTR 5510 SER 0C73243 OF 23MAY2000/-/-/X0//

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

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

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

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

EXHIBIT 6C

EQUIVALENT FOREIGN SECURITY CLASSIFICATIONS

| COUNTRY | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
|---|---|---|---|---|
| ALBANIA | TEPER SEKRET | SEKRET | IMIREBESUESHEM | I KUFIZUAR |
| ARGENTINA | ESTRICTAMENTE SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| AUSTRALIA | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| AUSTRIA | STRENG GEHEIM | GEHEIM | VERSCHLUSS | |
| BALKANS | STROGO POVERLJIVO<br>State SECRET<br>DRZAVA TAJNA | TAJNO<br>Military SECRET<br>VOJNA TAJNA | POVERLJIVO | |
| BELGIUM (French)<br><br>(Flemish) | TRES SECRET<br><br>ZEER GEHEIM | SECRET<br><br>GEHEIM | CONFIDENTIEL<br><br>VERTROUWELIJK | DIFFUSION RESTREINTS<br><br>BEPERTKE VERSPREIDING |
| BOLIVIA | SUPERSECRETO or MUY SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| BRAZIL | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| BULGARIA | STROGO SEKRENTO | SEKRETEN/ SEKRETNO | POVERITELEN/ POVERITELNO | OGRANICHE (as in limited)<br>NEPOZVOLEN (Illicit)<br>ZABRANEN (Forbiden) |
| CAMBODIA | TRES SECRET | SECRET | SECRET/ CONFIDENTIEL | |
| CANADA | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| CHILE | SECRETO | SECRETO | RESERVADO | RESERVADO |
| COLUMBIA | ULTRASECRETO | SECRETO | RESERVADO | CONFIDENCIAL RESTRINGIDO |
| COSTA RICA | ALTO SECRETO | SECRETO | CONFIDENCIAL | |
| CROATIA | NAJVECI TAJNITAJNI | TAJNI | POVERLJIV | OGRANCIEN |
| DENMARK | YDERST HEMMELIGT | HEMMELIGT | FORTROLIGT | TIL TJENESTEBRUG |
| ECUADOR | SECRETISIMO | SECRETO | CONFIDENCIAL | RESERVADO |
| EL SALVADOR | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |

| COUNTRY | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
|---|---|---|---|---|
| ETHIOPIA | YEMIAZ BIRTOU MISTIR | MISTIR | KILKIL | |
| FINLAND | ERITTAIN SALAINEN | | | |
| FRANCE | TRES SECRET | SECRET DEFENSE | CONFIDENTIEL | DIFFUSION RESTREINTE |
| GERMANY | STRENG GEHEIM | GEHEIM | VS-VERTRAULICH | |
| GREECE | | | | |
| GUATAMALA | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| HAITI | | SECRET | CONFIDENTIAL | |
| HONDURAS | SUPER SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| HONG KONG | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| HUNGARY | SZIGOR'UAN TITKOS | TITKOS | BIZALMAS | |
| ICELAND | ALGJORTI | TRUNADARMAL | | |
| INDIA | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| INDONESIA | SANGAT RAHASIA | RAHASIA | TERBATAS | |
| IRAN | BENKOLI SERRI | SERRI | KHEILI MAHRAMANEH | MAHRAMANEH |
| IRAQ (English Translation) | ABSOLUTELY SECRET | SECRET | | LIMITED |
| IRELAND (Gaelic) | AN-SICREIDEACH | SICREIDEACH | RUNDA | SRIANTA |
| ISRAEL | SODI BEYOTER | SODI | SHAMUR | MUGBAL |
| ITALY | SEGRETISSIMO | SEGRETO | RISERVATISSIMO | RISERVATO |
| JAPAN | KIMITSU | GOKUHI | HI | TORIATSUKAICHUI |
| JORDAN | MAKTUM JIDDAN | MAKTUM | SIRRI | MAHDUD |
| KAZAKSTAN | Use Russian Equivalent | Use Russian Equivalent | | |

| COUNTRY | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
|---|---|---|---|---|
| KOREA | I KUP PI MIL | II KUP PI MIL | III KUP PI MIL | |
| KYRGYZSTAN | Use Russian Equivalent | Use Russian Equivalent | | |
| LAOS | TRES SECRET | SECRET | SECRET/ CONFIDENTIEL | DIFFUSION RESTREINTE |
| LEBANON | TRES SECRET | SECRET | CONFIDENTIEL | |
| MOLDOVAN (May also use Russian equivalent) | ULTRASECRET | SECRET | CONFIDENTIAL OR SECRET | RESTRINS |
| MEXICO | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESTRINGIDO |
| NETHERLANDS | ZEER GEHEIM | GEHEIM | CONFIDENTIEEL OR VERTROUWELIJK | DIENSTGEHEIM |
| NEW ZEALAND | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| NICARAGUA | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| NORWAY | STRENGT HEMMELIG | HEMMELIG | KONFIDENSIELL | BEGRENSET |
| PAKISTAN | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| PARAGUAY | SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| PERU | ESTRICTAMENTE SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| PHILIPPINES | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| POLAND | TAIJNY SPECJALNEGO | TAJNY | POUFNY | |
| PORTUGAL | MUITO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| ROMANIA | ULTRASECRET | SECRET | CONFIDENTIAL OR SECRET | RESTRINS |
| RUSSIA | COBEOWEHHO | CEKPETHO | | |
| SAUDI ARABIA | SAUDI TOP SECRET | SAUDI VERY SECRET | SAUDI SECRET | SAUDI RESTRICTED |
| SPAIN | MAXIMO SECRETO | SECRETO | CONFIDENCIAL | DIFFUSION LIMITADA |
| SWEDEN (Red Borders) | HEMLIG (2 RED Borders) | HEMLIG (1 RED Border) | | |

| COUNTRY | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
|---|---|---|---|---|
| SWITZERLAND | (Three languages. TOP SECRET has a registration number to distinguish it from SECRET and CONFIDENTIAL) | | | |
| FRENCH | TRES SECRET | SECRET DEFENSE | CONFIDENTIEL DEFENSE | DIFFUSION RESTREINTE |
| GERMAN | STRENG GEHEIM | GEHEIM | VERTRAULICH | |
| ITALIAN | SEGRETISSIMO | SEGRETO | RISERVATISSIMO | RISERVATO |
| TAIWAN | (No translation in English characters) | | | |
| TAJIKISTAN | Use Russian Equivalent | Use Russian Equivalent | | |
| THAILAND | LUP TISUD | LUP MAAG | LUP | POK PID |
| TURKEY | COK GIZLI | GIZLI | OZEL | HIZMET OZEL |
| TURKMENISTAN | Use Russian Equivalent | Use Russian Equivalent | | |
| UKRAINE | TSILKOM SEKRETNE | SEKRETNO | KONFIDENTSIAL'NO | DLYA |
| UNION OF SOUTH AFRICA | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| AFRIKAANS | UITERS GEHEIM | GEHEIM | VERTROULIK | BEPERK |
| UNITED ARAB REPUBLIC (Egypt) | TOP SECRET | VERY SECRET | SECRET | OFFICIAL |
| UNITED KINGDOM | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| URUGUAY | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| UZBEKISTAN | Use Russian Equivalent | Use Russian Equivalent | | |
| VIET NAM (French) | TRES SECRET | SECRET DEFENSE | CONFIDENTIEL DEFENSE | DIFFUSION RESTREINTE |
| (VIETNAMESE) | TOI-MAT | MAT | KIN | TU MAT |

NOTE: The classifications given above represent the nearest comparable designation that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classification.

# CHAPTER 7

# SAFEGUARDING

## 7-1 BASIC POLICY

1. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited AISs, and under conditions which prevent unauthorized persons from gaining access. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified information is processed or stored. These areas may be designated, in writing, by the commanding officer as restricted areas per reference (a). Decisions regarding designations of restricted areas, their levels, and criteria for access are at the discretion of the commanding officer. All personnel shall comply with the **need-to-know** policy for access to classified information.

2. Classified information is the property of the U.S. Government and **not** personal property. Military or civilian personnel who resign, retire, separate from the DON, or are released from active duty, shall return all classified information in their possession to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers.

## 7-2 APPLICABILITY OF CONTROL MEASURES

Classified information shall be afforded a level of control commensurate with its assigned security classification level. This policy encompasses all classified information regardless of media.

## 7-3 TOP SECRET CONTROL MEASURES

1. All Top Secret information (including copies) originated or received by a command shall be continuously accounted for, individually serialized, and entered into a command Top Secret log. The log shall completely identify the information, and at a minimum include the date originated or received, individual serial numbers, copy number, title, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken.

2. In addition to the marking requirements of chapter 6, Top Secret information originated by the command shall be marked with an individual copy number in the following manner "Copy No. ____ of ____ copies." Exceptions to this rule are allowed for publications containing a distribution list by copy number and for mass-produced reproductions when copy numbering would be cost prohibitive. In the latter case, adequate and readily available documentation shall be maintained indicating the total copies produced and the recipients of the copies.

3. TSCOs shall obtain a record of receipt (typically a classified material receipt) from each recipient for Top Secret information distributed internally and externally.

4. Top Secret information shall be physically sighted or accounted for at least annually, and more frequently as circumstances warrant (e.g., at the change of command, change of TSCO, or upon report of loss or compromise). As an exception, repositories, libraries or activities which store large volumes of classified material may limit their annual inventory to all documents and material to which access has been given in the past 12 months, and 10 percent of the remaining inventory. See chapter 2, paragraph 2-3 for TSCO duties.

## 7-4 SECRET CONTROL MEASURES

Commanding officers shall establish administrative procedures for the control of Secret information appropriate to their local environment, based on an assessment of the threat, the location, and mission of their command. These procedures shall be used to protect Secret information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this regulation.

## 7-5 CONFIDENTIAL CONTROL MEASURES

Commanding officers shall establish administrative procedures for the control of Confidential information appropriate to their local environment, based on an assessment of the threat, location, and mission of their command. These procedures shall be used to protect Confidential information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this regulation.

## 7-6 WORKING PAPERS

1. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents. Working papers that contain classified information shall be:

a. Dated when created;

b. Conspicuously marked "Working Paper" on the first page in letters larger than the text;

c. Marked centered top and bottom on each page with the highest overall classification level of any information they contain;

d. Protected per the assigned classification level; and

e. Destroyed, by authorized means, when no longer needed.

2. Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

## 7-7 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. Control and safeguard special types of classified information as follows:

a. **NWPs**. Reference (b) requires an administrative system for controlling the NWP Library within the command. Classified NWPs shall be safeguarded per this chapter, according to their security classification level. Administrative controls for NWPs do not replace the security controls required for classified information.

b. **NATO**. Control and safeguard NATO classified information (including NATO Restricted) per reference (c).

c. **FGI.** Control and safeguard FGI, other than NATO, in the same manner as prescribed by this regulation for U.S. classified information, except as follows:

(1) FGI controls and safeguards may be modified as required or permitted by a treaty or international agreement, or by the responsible national security authority of the originating government for other obligations that do not have the legal status of a treaty or international agreement (e.g., a contract).

(2) **TOP SECRET FGI.** Maintain records for the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmission of Top Secret FGI. The originating government shall approve reproduction, and destruction shall be witnessed by two appropriately cleared personnel. Retain records for 5 years.

(3) **SECRET FGI.** Maintain records for the receipt, transmission and destruction of Secret FGI. Secret FGI may be reproduced to meet mission requirements and reproduction shall be recorded. Retain records for 3 years.

(4) **CONFIDENTIAL FGI.** Maintain records for the receipt and transmission of Confidential FGI. Other records need not be maintained unless required by the originating government. Retain records for 2 years.

(5) **FOREIGN GOVERNMENT RESTRICTED and UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE.** The degree of protection provided to the FGI shall be at least equivalent to that required by the foreign government. If the foreign government protection requirement is lower than the protection required for U.S. Confidential information observe the following rules:

(a) Provide the information only to those who have a need-to-know;

(b) Notify individuals given access of applicable handling instructions in writing or by an oral briefing; and

(c) Store information in a locked desk or cabinet, or in a locked room to which access is controlled to prevent unauthorized access.

d. **RD (INCLUDING CNWDI) and FRD.** Control and safeguard RD and FRD per reference (d).

e. **SCI.** Control and safeguard SCI per reference (e).

f. **COMSEC.** Control and safeguard COMSEC information per references (f) and (g).

g. **SIOP and SIOP-ESI.** Control and safeguard SIOP and SIOP-ESI per reference (h).

h. **SAPs.** Control and safeguard SAP information per reference (i).

i. **NNPI.** Control and safeguard NNPI per reference (j).

j. **FOUO.** Control and safeguard FOUO information per reference (k).

k. **SBU INFORMATION.** Control and safeguard SBU information in the same manner as FOUO, per reference (k).

l. **DEA SENSITIVE INFORMATION.** Control and safeguard DEA Sensitive information in the same manner as FOUO, per reference (k).

m. **DoD UCNI.** Control and safeguard DoD UCNI per reference (l).

n. **SENSITIVE INFORMATION (COMPUTER SECURITY ACT OF 1987).** Control and safeguard Sensitive Information contained in U.S. Government AISs per reference (m).

## 7-8 ALTERNATIVE OR COMPENSATORY CONTROL MEASURES

1. The CNO (N09N) approves the use of alternative or compensatory security control measures and ensures that the protection afforded classified information is sufficient to reasonably deter and detect loss or compromise. Upon request, OCAs shall furnish to other DoD components or executive branch agencies, with whom classified information or secure facilities are shared, approvals for alternative or compensatory control measures. The CNO (N09N2) will provide a copy of this documentation to the DUSD(PS) or ASD($C^3I$) as appropriate, for reporting to the Director, ISOO.

2. Requests for approval of such controls shall include criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and countermeasures benefits versus cost.

3. The CNO (N09N2) shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for their use. Controls include:

a. Maintenance of lists or rosters of personnel to whom the classified information has been or may be provided;

b. Using a nickname to identify classified information which requires alternative or compensatory protection. A code word shall not be used for this purpose. Other special terminology or special markings shall not be used except that prescribed for the handling of messages.

c. Requiring that classified information be placed in sealed envelopes marked only with the nickname and stored in a manner to avoid combining with other classified information.

d. Requiring unique DoD component oversight or inspection procedures.

4. Approved controls may be applied to cleared DoD contractors only when identified in the DD 254.

5. Alternative or compensatory security control measures shall not be applied to RD (including CNWDI), FRD, SIOP or SIOP-ESI information.

6. Requests to use alternative or compensatory security control measures for the safeguarding of NATO or FGI shall be submitted to the DUSD(PS) via the administrative chain of command and the CNO (N09N2).

7. Alternative or compensatory security control measures shall not preclude, nor unnecessarily impede, Congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

**7-9 CARE DURING WORKING HOURS**

1. Keep classified information under constant surveillance by an authorized person or covered with SFs 703, 704, or 705 when removed from secure storage.

2. In a mixed working environment (i.e., classified and unclassified), AIS media used for processing or storing classified information shall be marked with an SF 706, 707,

708, 709, 710, 711, or 712 (SCI), as applicable. In a totally unclassified working environment, SF labels are not required.

3. Protect preliminary drafts, plates, stencils, stenographic notes, worksheets, computer printer and typewriter ribbons, computer storage media, and other classified items according to their security classification level. Immediately destroy these items after they have served their purpose.

4. Classified discussions shall not be conducted with or in the presence of unauthorized persons. Take special care when visitors are present. Practice the need-to-know principle.

## 7-10 END-OF-DAY SECURITY CHECKS

Commanding officers shall establish procedures for end of the day security checks, utilizing the SF 701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, an SF 702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms (strong rooms), and containers have been properly secured at the end of the day. The SF 701 and 702 shall be annotated to reflect after hours, weekend, and holiday activities in secure areas.

## 7-11 SAFEGUARDING DURING VISITS

Commanding officers shall establish procedures to ensure that only visitors with an appropriate clearance level and need-to-know are granted access to classified information. At a minimum, these procedures shall include verification of the identity, clearance level, access (if appropriate), and need-to-know for all visitors. Refer to reference (n) for visit procedures.

## 7-12 SAFEGUARDING DURING CLASSIFIED MEETINGS

1. Commanding officers shall ensure that classified discussions at conferences, seminars, exhibits, symposia, conventions, training courses, or other gatherings (hereafter referred to as "meetings") are held only when disclosure of the information serves a specific U.S. Government purpose. Classified meetings shall be held only at a U.S. Government agency or a cleared DoD contractor facility with an appropriate facility security clearance (FCL) where adequate physical security and procedural controls have been approved.

2. Commands hosting in-house meetings attended by members of the command and authorized visitors shall assume security responsibility for the meeting. Take precautions for conference rooms and areas specifically designated for classified discussions. Request technical surveillance counter-measures support for conferences involving Top Secret information, and for other designated classified discussion areas per reference (o).

3. Commands hosting meetings outside the command, including those supported by non-U.S. Government associations, shall:

a. Confirm that other means for communicating or disseminating the classified information in lieu of a meeting are inadequate;

b. Ensure that attendance is limited to U.S. Government personnel or cleared DoD contractor employees. Any participation by foreign nationals or foreign representatives shall be approved, in writing, by the DON command foreign disclosure office or Navy IPO prior to attendance to ensure that the information to be presented has been cleared for foreign disclosure. All attendees shall possess an appropriate level of clearance and need-to-know;

c. Prepare and implement a security plan that minimizes the risk to the classified information involved;

d. Segregate classified sessions from unclassified sessions;

e. Ensure that announcements are unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions when non-U.S. Government associations are providing administrative support;

f. Permit note taking or electronic recording during classified sessions only when the sponsor determines, in writing, that such action is necessary to fulfill the U.S. Government purpose for the meeting; and

g. Safeguard, transmit, or transport classified information created, used, or distributed during the meeting per this chapter and chapter 9.

4. Command personnel invited to give classified presentations or to accept security sponsorship for classified meetings organized by non-U.S. Government associations must receive approval from

the CNO (N09N2) prior to any commitment or announcement being made. Requests to conduct such meetings shall be forwarded to the CNO (N09N2) via the administrative chain of command and shall include:

a. A summary of subjects, level, and sources of classified information;

b. The name of the non-U.S. Government association or organization involved in the meeting;

c. The location and dates of the meeting;

d. Identification of the sponsoring command, including the name, address, and phone number of the primary action officer;

e. The specific reason for having the meeting;

f. A security plan specifying procedures for processing security clearances, badging procedures, access control procedures, and procedures for storing the classified information;

g. A draft agenda, announcement, and clearance verification form;

h. The identity of any foreign representatives expected to attend, with proof of their official clearance level assurance and a statement of their need-to-know.

5. Pending a decision by the CNO (N09N2), general notices or announcements of meetings may be published or sent to members of participating associations, societies, or groups if the notice or announcement does not constitute an invitation to attend. If approval is granted, the CNO (N09N2) shall appoint a U.S. Government official to serve as security manager for the meeting. The security manager shall provide and maintain physical security for the actual site of the classified meeting. Other U.S. Government organizations or cleared contractor facilities with an appropriate level FCL may assist with implementation of security requirements under the direction of the appointed security manager. Upon assuming security sponsorship, the sponsor shall review all announcements and invitations to determine that they are accurate, do not contain classified information, and clearly identify the security sponsor.

## 7-13 REPRODUCTION

1. U.S. classified and DEA Sensitive unclassified information shall be reproduced only to the extent required by operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives. See paragraph 7-7.3 for reproduction of FGI.

2. Commanding officers shall:

a. Designate specific equipment for classified reproduction;

b. Limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk;

c. Comply with reproduction limitations placed on classified information by originators and special controls applicable to special types of classified information;

d. Facilitate oversight and control of reproduction; and

e. Ensure the expeditious processing of classified information in connection with review for declassification.

### REFERENCES

(a) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98 (NOTAL)

(b) NWP 1-01, *Naval Warfare Publications System*, Hardcopy Nov 1994/CD-ROM Dec 97 (NOTAL)

(c) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(d) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(e) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(f) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(g) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

(h) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(i) OPNAVINST S5460.4C, *Control of Special Access Programs Within the DON (U)*, 14 Aug 81 (NOTAL)

(j) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(k) SECNAVINST 5720.42E, *DON Freedom of Information Act, (FOIA) Program*, 5 Jun 91

(l) OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI)*, 11 Feb 93

(m) Title 5 of Public Law 93-579, *The Privacy Act*, U.S.C., Section 552a

(n) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(o) SECNAVINST 5500.31A, *Technical Surveillance Countermeasures (TSCM) Program*, 4 Jun 85 (NOTAL)

# CHAPTER 8

# DISSEMINATION

## 8-1 BASIC POLICY

1. Commanding officers shall establish procedures for the dissemination of classified and controlled unclassified information originated or received by their command.

2. Classified information originated in a non-DoD department or agency shall not be disseminated outside the DoD without the consent of the originator, except where specifically permitted.

3. Authority for disclosure of classified information to foreign governments has been centralized in the Director, Navy IPO who has delegated authority to disclose certain classified information to those commands designated in reference (a).

## 8-2 TOP SECRET

Top Secret information originated within the DoD shall not be disseminated outside the DoD without the consent of the originator or higher authority.

## 8-3 SECRET AND CONFIDENTIAL

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

## 8-4 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. **SAPs.** The policy and procedures concerning the dissemination of SAP information are contained in reference (b).

2. **RD (including CNWDI) and FRD.** The policy and procedures concerning access to and dissemination of RD (including CNWDI) and FRD within the DoD are contained in references (c) and (d).

3. **NATO.** The policies and procedures for the dissemination of NATO information are contained in reference (e). DON documents which incorporate NATO information do not require transmission through NATO channels.

4. **COMSEC.** The policies and procedures for the dissemination of COMSEC information are contained in reference (f).

5. **SCI.** The policies and procedures for the dissemination of SCI are contained in reference (g).

6. **SIOP and SIOP-ESI.** The policies and procedures for the dissemination of SIOP and SIOP-ESI are contained in reference (h).

7. **NNPI.** The policies and procedures for the dissemination of NNPI, U-NNPI and DOE Unclassified Controlled Nuclear Information (DOE UCNI) are contained in reference (i).

8. **FOUO.** The policies and procedures for the dissemination of FOUO information are contained in reference (j). FOUO information may be disseminated within the DoD components and between officials of the DoD components, cleared DoD contractors, consultants, and grantees in the conduct of official business for the DoD and DON. FOUO information may be released to other DoD departments and agencies of the U.S. Government as necessary in the conduct of valid official business and shall be marked per chapter 6, paragraph 6-11.3a. Reference (j) also establishes the policy governing the release of FOUO information to members of Congress and General Accounting Office (GAO) personnel.

9. **SBU INFORMATION.** The policies and procedures for the dissemination of SBU are the same as those used for FOUO information, reference (j).

10. **DEA SENSITIVE INFORMATION.** DEA Sensitive information is unclassified information that is originated by the DEA and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. Access to DEA Sensitive information shall be granted only to persons who have a valid need-to-know. DEA Sensitive information shall not be released outside the DoD without DEA authorization.

11. **DoD UCNI.** DoD UCNI is unclassified information on security measures (including security plans, procedures and equipment) for physical protection of DoD Special Nuclear Material, equipment, or facilities. Access to DoD UCNI shall be granted only to persons who have a valid need-to-know and are specifically eligible for access under the provisions of reference (k).

12. **SENSITIVE INFORMATION (COMPUTER SECURITY ACT OF 1987).** The Computer Security Act of 1987 established requirements for protection of certain information in U.S. Government AISs. This information is referred to as sensitive information and defined as "information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under reference (l), but which has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept Secret in the interest of national defense or foreign policy." Access to this information shall be limited only to those with a valid need-to-know.

## 8-5 DISSEMINATION OF INTELLIGENCE INFORMATION

The Director of Central Intelligence has provided controlled relief to the "third agency rule" by authorizing members of the Intelligence Community to use each other's classified intelligence in their intelligence documents, publications and other information media and to disseminate their products to other Intelligence Community organizations, subject to the limitations and procedures described in reference (m).

## 8-6 DISSEMINATION TO CONGRESS

The policies and procedures for the preparation and processing of classified information to be disseminated to Congress are contained in references (n) and (o).

## 8-7 DISSEMINATION OF TECHNICAL DOCUMENTS

1. Reference (p) requires the assignment of distribution statements to facilitate control, distribution, and release of documents without the need to repeatedly refer questions to the originating command. The originating command may choose to make case-by-case exceptions to distribution limitations imposed by the statement. Distribution statements also provide the extent of secondary distribution that is permissible without further authorization or approval of the originating command.

2. All newly generated DoD unclassified technical documents shall bear one of the distribution statements described in **exhibit 8A**. If not already in the public domain and likely to be disseminated outside the DoD, existing unclassified technical documents, including informal documents such as working papers, memoranda, and preliminary reports shall be assigned a distribution statement from **exhibit 8A**. Existing technical documents do not have to be reviewed for the sole purpose of

assigning distribution statements but, when they are removed from files, a determination shall be made whether distribution limitations are necessary and, if so, they must be marked accordingly.

3. Classified technical documents shall be assigned Distribution Statements B, C, D, E, or F from **exhibit 8A**. The distribution statement assigned to a classified document shall be retained on the document after its declassification or until specifically changed or removed by the originating command. Technical documents that are declassified and have no distribution statement assigned shall be handled per Distribution Statement F until changed by the originating command.

4. Information relating to NNPI which is not marked and handled as unclassified NNPI shall be reviewed and approved by the Naval Sea Systems Command (SEA-08) prior to release to the public.

5. This policy covers all newly created technical documents generated by all DoD-funded RDT&E programs which are the basis of the Navy Scientific and Technical Information Program described in reference (q). It applies to newly created engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment.

6. Reference (r) applies to unclassified technical data which reveals critical technology with military or space application and requires an approval, authorization, or license for its lawful export and which may be withheld from public disclosure (officially released under proper authority). This withholding authority does not apply to scientific, educational, or other data not directly and significantly related to design, production, or utilization in industrial processes.

**8-8 PREPUBLICATION REVIEW**

Reference (s) applies to public affairs and reference (t) applies to the clearance of DoD information for public release. Reference (u) establishes the policy that a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on electronic bulletin boards accessible through the INTERNET or publicly accessible computer servers. **Exhibit 8B** is an excerpt from reference (u) identifying official DoD

information prepared by or for DoD personnel and proposed for public release that requires a review by the Assistant Secretary of Defense, Public Affairs (ASD(PA)) via the CNO (N09N2).

## REFERENCES

(a) SECNAVINST 5510.34, *Manual for the Disclosure of DON Military Information to Foreign Governments and International Organizations*, 4 Nov 93

(b) OPNAVINST S5460.4C, *Control of Special Access Programs Within DON (U)*, 14 Aug 81 (NOTAL)

(c) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(d) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(e) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(f) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(g) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(h) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(i) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(j) SECNAVINST 5720.42E, *DON Freedom of Information Act (FOIA) Program*, 5 Jun 91

(k) OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI)*, 11 Feb 93

(l) Title 5 of Public Law 93-579, *The Privacy Act*, (U.S.C., Section 552a)

(m) DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*, 30 Jun 98 (NOTAL)

(n) SECNAVINST 5730.5G, *Procedures for the Handling of Naval Legislative Affairs and Congressional Relations*, 24 Aug 81

(o) OPNAVINST 5510.158A, *Security Review Guide for Congressional Matters*, 10 Dec 84 (NOTAL)

(p) DoD Directive 5230.24, *Distribution Statements on Technical Documents*, 18 Mar 87 (NOTAL)

(q) SECNAVINST 3900.43A, *Navy Scientific and Technical Information Program*, 20 Jul 94 (NOTAL)

(r) OPNAVINST 5510.161, *Withholding of Unclassified Technical Data from Public Disclosure*, 29 Jul 85

(s) SECNAVINST 5720.44A, *DON Public Affairs Regulations*, 3 Jun 87

(t) DoD Directive 5230.9, *Clearance of DoD Information for Public Release*, 9 Apr 96

(u) DoD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, 6 May 96

# EXHIBIT 8A

## PROCEDURES FOR ASSIGNING DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS

1. Newly generated unclassified technical documents shall be assigned Distribution Statements A, B, C, D, E, F, or X. If not already in the public domain and are likely to be disseminated outside the DoD, existing unclassified technical documents shall be assigned Distribution Statements A, B, C, D, E, F, or X.

2. Technical documents in preliminary or working draft form shall not be disseminated without a proper security classification review and assignment of a distribution statement.

3. Classified technical documents shall be assigned Distribution Statements B, C, D, E, or F. The distribution statement assigned to a classified document shall be retained on the document after declassification or until specifically changed or removed by the originating command. If a technical document without a distribution statement is declassified, it shall be handled as a Distribution Statement F document until otherwise notified by the originating command.

4. If a newly generated technical document contains export-controlled technical data, it shall be marked with the statement in paragraph 1 under "ADDITIONAL NOTICES," in addition to Distribution Statements B, C, D, E, F, or X.

5. Scientific and technical documents which include a contractor-imposed "limited rights" statement shall be appropriately marked and controlled (see "CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS" below).

6. The distribution statement shall be displayed conspicuously so it is readily recognized by recipients. For standard written or printed material, the distribution statement shall appear on the face of the document, title page, and DD 1473, "Report Documentation Page." When possible, parts that contain information creating the requirement for the distribution statement shall be prepared as an appendix to permit broader distribution of the basic document. When practicable, the abstract of the document, the DD 1473, and bibliographic citations shall be written in such a way that the information shall not be subject to Distribution Statements 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 shall be conspicuously stamped, printed, or written by other means.

7. Distribution statements remain in effect until changed or removed by the originating command. Each command shall 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 shall be processed per DoD Instruction 5230.29 of 6 May 1996 (NOTAL). When public release clearance is obtained, Distribution Statement A shall be assigned and document handling facilities, including the Defense Technical Information Center (DTIC), shall be notified.

8. Technical documents with superseded distribution limitation markings shall be reviewed and assigned the appropriate distribution statement when a request for the document is received. Superseded distribution limitation markings shall be converted as follows:

a. Documents with distribution marking A or B need not be reevaluated or remarked.

b. Documents with distribution marking #2 shall be assigned Distribution Statement C.

c. Documents with distribution marking #3 (U.S. Government Only) shall be assigned Distribution Statement B.

d. Documents with distribution marking #4 (DoD Only) shall be assigned Distribution Statement E.

e. Documents with distribution marking #5 (Controlled) shall be assigned Distribution Statement F.

9. Originating commands shall promptly notify DTIC and other information repositories holding their technical documents when:

a. The 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

1. The following distribution statements are authorized for use on technical documents:

a. **"DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited."**

(1) This statement shall be used only on unclassified technical documents that have been cleared for public release by competent authority per DoD Instruction 5230.29 (NOTAL) and DoD Directive 5230.9 of 9 April 1996 (NOTAL).

(2) Technical documents resulting from contracted fundamental research efforts shall 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.

(3) Technical documents with this statement may be made available or sold to the public including foreign nationals, companies, and governments, and may be exported.

(4) This statement shall 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.

(5) This statement shall not be used on classified technical documents or documents containing export-controlled technical data as provided in OPNAVINST 5510.161 of 29 July 1985.

b. **"DISTRIBUTION STATEMENT B: Distribution authorized to U.S. Government agencies only; (fill in reason) (date). Other requests for this document shall be referred to (insert originating command)."**

(1) This statement shall be used on unclassified or 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.

(2) Reasons for assigning Distribution Statement B include:

(a) FGI - To protect and limit information distribution per the desires of the foreign government that furnished the technical information. Information of this type is normally classified at the Confidential level or higher.

(b) 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.

(c) 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 of 29 July 1985.

(d) Test and 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.

(e) Contractor Performance Evaluation - To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

(f) Premature Dissemination - To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.

(g) Administrative/Operational Use - To protect technical or operational 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 shall be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

(h) Software Documentation - Releasable only per the provisions of DoD Instruction 7930.2 of 31 December 1979 (NOTAL).

(i) Specific Authority - To protect information not specifically included in the above reasons and discussions, but which requires protection per valid documented authority such as E.O.s, classification guidelines, DoD or DON regulations, or policy guidance. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

c. **"DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors; (fill in reason) (date). Other requests for this document shall be referred to (insert originating command)."**

(1) May be used on unclassified or 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.

(2) Reasons for assigning Distribution Statement C include:

(a) FGI - Same as Distribution Statement B.

(b) Critical Technology - Same as Distribution Statement B.

(c) Software Documentation - Same as Distribution Statement B.

(d) Administrative or Operational Use - Same as Distribution Statement B.

(e) Specific Authority - Same as Distribution Statement B.

d. **"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)."**

(1) May be used on unclassified or 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.

(2) Reasons for assigning Distribution Statement D include:

(a) FGI - Same as Distribution Statement B.

(b) Administrative or Operational Use - Same as Distribution Statement B.

(c) Software Documentation - Same as Distribution Statement B.

(d) Critical Technology - Same as Distribution Statement B.

(e) Specific Authority - Same as Distribution Statement B.

e. **"DISTRIBUTION STATEMENT E: Distribution authorized to DoD Components only; (fill in reason) (date). Other requests shall be referred to (insert originating command)."**

(1) May be used on unclassified or 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.

(2) Reasons for assigning Distribution Statement E include:

(a) 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 U.S. Designation of such data is made by competent authority per OPNAVINST 5510.161 of 29 July 1985.

(b) FGI - Same as Distribution Statement B.

(c) Proprietary Information - Same as Distribution Statement B.

(d) Premature Dissemination - Same as Distribution Statement B.

(e) Test and Evaluation - Same as Distribution Statement B.

(f) Software Documentation - Same as Distribution Statement B.

(g) Contractor Performance and Evaluation - Same as Distribution Statement B.

(h) Critical Technology - Same as Distribution Statement B.

(i) Administrative/Operational Use - Same as Distribution Statement B.

(j) Specific Authority - Same as Distribution Statement B.

f. **"DISTRIBUTION STATEMENT F: Further dissemination only as directed by (insert originating command) (date) or higher DoD authority."**

(1) Normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists.

(2) Distribution Statement F is used when the originator determines that the information is subject to the special dissemination limitation specified in chapter 6, paragraph 6-11.3a.

(3) When a classified document assigned Distribution Statement F is declassified, the statement shall be retained until specifically changed or removed by the originating command.

g. **"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. Other requests shall be referred to (originating command)."**

(1) This statement shall be used on unclassified documents when Distribution Statements B, C, D, E, or F are not applicable but the document contains technical data per OPNAVINST 5510.161 of 29 July 1985.

(2) This statement shall not be used on classified technical documents. It may be assigned to technical documents that formerly were classified.

## ADDITIONAL NOTICES

1. In addition to the distribution statement, the following notices shall be used when appropriate:

a. All technical documents determined to contain export-controlled technical data shall 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 per the provisions of OPNAVINST 5510.161." When it is technically impracticable to use the entire statement, an abbreviated marking shall 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 of 29 July 1985.

2. Unclassified/Limited Distribution documents shall be handled using the same standard as FOUO information, and shall 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 U.S. Government is given limited rights. The contractor shall place a limited rights statement on each document containing contractor controlled technical data furnished to the U.S. Government. Documents with limited rights information shall 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 express limitation that such technical data, without the written permission of the party furnishing the technical data, shall not be:

a. Released or disclosed in whole or in part outside the U.S. Government.

b. Used in whole or in part by the U.S. 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 U.S. Government, except for:

(1) Emergency repair or overhaul work only by or for the U.S. 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 U.S. 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 U.S. Government 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) above.

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 the appropriate distribution statement.

## EXHIBIT 8B

## CATEGORIES OF INFORMATION WHICH REQUIRE REVIEW AND CLEARANCE BY THE ASD(PA) PRIOR TO PUBLIC RELEASE

1. Certain categories of information require review and clearance by the ASD(PA) via the CNO (N09N2) before public release. They include information which:

a. Originates or is proposed for public release in the Washington, D.C. area;

b. Is or has the potential to become an item of national or international interest;

c. Affects national security policy or foreign relations;

d. Concerns a subject of potential controversy among the DoD components or with other federal agencies;

e. Is presented by a DoD employee, who by virtue of rank, position, or expertise would be considered an official DoD spokesperson;

f. Contains technical data, including data developed under contract or independently developed and controlled by the International Traffic in Arms Regulation (ITAR), that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made; or,

g. Bears on any of the following subjects:

(1) New weapons or weapons systems, significant modifications or improvements to existing weapons, weapons systems, equipment, or techniques.

(2) Military operations, significant exercises, and operations security.

(3) National Command Authorities; command, control, communications, computers, and intelligence; information warfare; and computer security.

(4) Military activities or application in space; nuclear weapons, including nuclear weapons effects research; chemical warfare and defensive biological warfare; and arms control treaty implementation.

# CHAPTER 9

# TRANSMISSION AND TRANSPORTATION

## 9-1 BASIC POLICY

1. Commanding officers shall ensure that only appropriately cleared personnel or carriers transmit, transport, escort, or handcarry classified information. Unless a specific kind of transmission or transportation is restricted, the means selected should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.

2. All international transfers of classified information shall take place through government-to-government channels. Follow the provisions of exhibit 9A.

## 9-2 TOP SECRET

Transmit or transport U.S. Top Secret information only by:

1. Direct contact between appropriately cleared U.S. personnel;

2. The Defense Courier Service (DCS), if qualified under the provisions of reference (a);

3. The DOS Diplomatic Courier Service;

4. Communications protected by a cryptographic system authorized by the Director, NSA or a protected distribution system designed and installed to meet the requirements of reference (b). (This applies to voice, data, message, and facsimile transmissions);

5. Appropriately cleared DoD contractor employees or U.S. military or Government civilian personnel specifically designated to escort or handcarry the information, traveling on a conveyance owned, controlled, or chartered by the U.S. Government traveling by surface transportation;

6. Appropriately cleared U.S. military or Government civilian personnel, specifically designated to escort or handcarry classified information, traveling on scheduled commercial passenger aircraft within and between the U.S., its territories, and Canada;

7. Appropriately cleared U.S. military and Government civilian personnel, specifically designated to escort or handcarry classified information, traveling on scheduled commercial passenger aircraft on flights outside the U.S., its territories, and Canada per paragraph 9-12; and

8. Appropriately cleared and designated DoD contractor employees within and between the U.S., its territories, and Canada per reference (c).

**9-3 SECRET**

Transmit or transport U.S. Secret information only by:

1. Any means approved for Top Secret information, except that Secret information may be introduced into the DCS only when U.S. control cannot otherwise be maintained. This restriction does not apply to COMSEC and SCI, per paragraph 9-5;

2. US Postal Service (USPS) registered mail within and between the U.S. and its territories;

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

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

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

6. U.S. Government and Government contract vehicles including aircraft and ships of the U.S. Navy, civil service-operated U.S. Naval Ships (Military Sealift Command), and ships of U.S. registry. Appropriately cleared operators of vehicles, officers

of ships, and pilots of aircraft who are U.S. citizens 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 observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible to unauthorized persons or is in a specialized secure, safe-like container;

7. The current holder of the General Services Administration (GSA) contract for overnight delivery, when approved by the official command mail control officer. Use of this service is on an exception basis, when applicable postal regulations are met, and when an urgent requirement exists for overnight delivery for the executive branch to a DoD component or to a cleared DoD contractor facility within the U.S. and its territories. The delivery service shall be U.S.-owned and U.S.-operated, provide automated in-transit tracking, and ensure package integrity during transit. The contract shall require cooperation with U.S. Government inquiries in the event of a loss or possible compromise. Size and weight limitations shall be met. The sender shall ensure that an authorized person is available to receive the delivery and shall verify the correct mailing address. Under no circumstances shall the release signature block on the receipt label be executed. The use of external (street-side) collection boxes is prohibited. Classified COMSEC, NATO, and FGI shall not be transmitted in this manner;

8. Carriers cleared under the NISP who provide a Protective Security Service (PSS). This method is authorized only within the Continental U.S. (CONUS) when other methods are impractical, except that this method is also authorized between U.S. and Canadian government-approved locations documented in a transportation plan approved by the U.S. and Canadian government security authorities;

9. In the hold of a cleared U.S. registered air carrier (Civilian Reserve Air Fleet Participant) without an appropriately cleared escort, in exceptional circumstances with the written approval of the recipient government security authorities. The shipment shall be sent between two specific points with no intermediate stops. The carrier shall agree in advance to permit cleared and specifically authorized persons to observe placement and removal of the classified shipment from the air carrier. The shipment shall be placed in a compartment that is not accessible to unauthorized persons or shall be placed in the same type of specialized shipping container prescribed for use by the DCS.

## 9-4 CONFIDENTIAL

Transmit or transport U.S. Confidential information only by:

1. Any means approved for Secret information;

2. USPS registered mail to and from APO or FPO addressees located outside the U.S. and its territories, and when the originator is uncertain that the addressees location is within U.S. boundaries;

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

4. USPS first class mail between DoD component locations anywhere in the U.S. and its territories. The outer envelope or wrapper shall be endorsed: "RETURN SERVICE REQUESTED".

5. A carrier that provides Constant Surveillance Service (CSS) within CONUS. A cleared DoD contractor facility shall be notified by separate communication at least 24 hours in advance of the shipment arrival. Information about commercial carriers providing a CSS is available from the Military Traffic Management Command (MTMC).

6. Personal custody of commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry shall not pass out of U.S. Government control. The commanders or masters shall receipt for the cargo and agree to:

a. Deny access to the Confidential information by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspections shall not be unloaded; and

b. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

## 9-5 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. **COMSEC.** References (d) and (e) establish the requirements for the transmission or transportation of COMSEC information.

2. **NATO.** Reference (f) establishes the requirements for the transmission or transportation of classified NATO information. NATO RESTRICTED information shall, at a minimum, be transmitted by USPS first class mail within CONUS and USPS first class mail using an APO/FPO address outside CONUS (single wrapped). Geographical addresses and international mail channels shall not be used.

3. **SCI.** Reference (g) establishes the requirements for the transmission or transportation of SCI.

4. **SAPs.** Reference (h) establishes the requirements for the transmission or transportation of SAP information.

5. **SIOP and SIOP-ESI.** Reference (i) establishes the requirements for the transmission or transportation of SIOP and SIOP-ESI.

6. **NNPI.** The policies and procedures for the transmission or transportation of NNPI, U-NNPI, and DOE UCNI are contained in reference (l). Since there is foreign national access to the internet, U-NNPI may only be transmitted on the internet if the transmission is encrypted. The encryption standard for transmission of U-NNPI is Federal Information Processing Standards (FIPS) 140-1.

7. **RD (including CNWDI) and FRD.** Transmit or transport RD (including CNWDI) and FRD in the same manner as other classified information of the same security classification. Reference (j) establishes the requirements for the transmission or transportation of nuclear information or components.

8. **FOUO.** Transport FOUO information via USPS first class mail, or standard mail for bulk shipments. Electronic transmission of FOUO information (voice, data, or facsimile) shall be by approved secure communications systems whenever practical. All means used shall preclude unauthorized public disclosure per reference (k).

9. **SBU (formerly LOU).** Transmit or transport DOS SBU information in the same manner as FOUO information.

10. **DEA SENSITIVE INFORMATION.** Transmit or transport DEA Sensitive information within CONUS by USPS first class mail. Transmit or transport DEA Sensitive information outside the CONUS (double wrapped and marked on both sides of the inner envelope with "DEA Sensitive") by any means approved for the transmission

or transportation of Secret material (see paragraph 9-3). Non-Government package delivery and courier services shall not be used. Electronic transmission of DEA Sensitive information within CONUS and outside CONUS shall be over approved secure communications circuits.

11. **DoD UCNI.** Transmit or transport DoD UCNI via USPS first class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DoD UCNI shall be over approved secure communications circuits per reference (m).

12. **SENSITIVE INFORMATION (COMPUTER SECURITY ACT of 1987).** Reference (n) establishes the requirements for the transmission of sensitive information in AISs.

13. **FOREIGN GOVERNMENT RESTRICTED and UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE.** Transmit or transport in a method approved for classified information, unless this method is waived by the originating government.

## 9-6 TELEPHONE TRANSMISSION

Classified telephone conversations shall be permitted only over secure communication circuits approved for the classification level of the information being discussed. Every attempt shall be made to ensure that the classified information is not compromised to unauthorized personnel.

## 9-7 CLASSIFIED BULKY FREIGHT SHIPMENTS

Commanding officers shall establish procedures for shipping bulky classified information as freight. These procedures shall include provisions for shipment in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and actions to be taken in case of non-delivery or unexpected delay in delivery.

## 9-8 PREPARING CLASSIFIED INFORMATION FOR SHIPMENT

1. Prepare classified information for shipment by packaging and sealing it with tape which will retain the impression of any postal stamp, in ways that minimize risk of accidental exposure or undetected deliberate compromise. Classified information shall be packaged so that classified text is not in direct contact with the inner envelope or container.

2. Enclose classified information transported outside the command in two opaque, sealed covers (e.g., envelopes, wrappings, or containers) durable enough to conceal and protect it from inadvertent exposure or tampering. The following exceptions apply:

a. If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner cover provided it does not reveal any classified information.

b. If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient cover provided observation does not reveal classified information.

c. If the classified information is an item of equipment that is not reasonably packageable and the shell or body is classified, it shall be concealed with an opaque covering that conceals all classified features.

d. Specialized shipping containers, including closed cargo transporters, may be considered the outer wrapping or cover when used.

e. Refer to the appropriate reference in paragraph 9-5 for preparation of special types of classified and controlled unclassified information for transmission or transportation.

**9-9 ADDRESSING CLASSIFIED INFORMATION FOR SHIPMENT**

1. Address the outer envelope or container only to an official U.S. Government activity or a cleared DoD contractor facility with the appropriate FCL level and storage capability. Include the complete return address of the sender. The outer envelope or container shall not have any markings indicating, or alerting handlers to the classification level of the contents. The classified information shall not be addressed to an individual (except when using USPS Express Mail or the current holder of the GSA contract for overnight delivery); however, an attention line may be used to include an office code or a specific department to aid in internal routing. Classified information intended only for U.S. elements of international staffs or other organizations shall be addressed specifically to those elements.

2. The **inner envelope or container** shall show the address of the recipient, the address of the sender, the highest classification level of the contents (including all warning notices, intelligence control markings, or any other applicable special instructions (see chapter 6, paragraphs 6-11 and 6-12)), and may also include an "attention line" with the intended recipient's name and/or office code.

3. Refer to the appropriate reference in paragraph 9-5 on addressing special types of classified and controlled unclassified information for transmission or transportation.

4. **DOS Diplomatic Courier Service.** The outer envelope of the classified information to be sent through the DOS Diplomatic Courier Service shall be addressed to: Chief, Classified Pouch and Mail Branch, U.S. Department of State, Washington, DC 20520-0528 and mailed via USPS registered mail. Mark the inner envelope with the appropriate classification level and address of the specific overseas activity.

5. **USPS Express Mail.** The USPS Express Mail envelope may serve as the outer wrapper.

6. **Current Holder of GSA Contract for Overnight Delivery.** The delivery envelope may serve as the outer wrapper and may be addressed to the recipient by name.

## 9-10 RECEIPTING FOR CLASSIFIED INFORMATION

1. Acknowledgement of receipt is required for Top Secret and Secret information transmitted or transported in and out of the command and for all classified information provided to a foreign government or its representatives, including its embassies in the U.S., and its contractors. A receipt is required with all classified packages handcarried to the U.S. Senate.

2. Use OPNAV 5511/10, Record of Receipt (**exhibit 9B**), and attach it to the inner cover. The receipt shall contain only unclassified information that clearly identifies the classified information. Retain Top Secret receipts for 5 years and Secret receipts for 2 years (see chapter 7, paragraph 7-7 for receipt retention of FGI). Failure to sign and return a receipt to the sender may result in a report of possible loss or compromise.

## 9-11 GENERAL PROVISIONS FOR ESCORTING OR HANDCARRYING CLASSIFIED INFORMATION

1. Use a cover sheet, file folder, or other covering to prevent inadvertent disclosure when handcarrying classified information within the command.

2. Double-wrap the classified information when handcarrying outside the command. A locked briefcase may serve as the outer cover, except when handcarrying aboard commercial aircraft. When handcarrying classified information to another command, refer to the provisions of this chapter on requirements for receipting, addressing, and covering.

3. Second echelon commands shall approve escorting or handcarrying of classified information aboard commercial aircraft traveling outside the U.S., its territories, and Canada. This authority may be further delegated, in writing, to subordinate commands as necessary.

4. Commanding officers or other designated officials shall authorize official travelers to escort or handcarry classified information only when:

a. The information is not available at the destination and is needed for operational necessity or a contractual requirement;

b. The information cannot be transmitted via a secure facsimile or other secure means in sufficient time for the stated purpose;

c. The escort or handcarry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available and the information remains in the custody and physical control of the U.S. courier or escort at all times; and

d. Advance arrangements have been made for secure storage at a U.S. embassy, military or cleared DoD contractor facility with safeguarding capability, commensurate with the classification level of the handcarried information, at the destination and all intermediate stops.

5. Commanding officers shall ensure that couriers are informed of and acknowledge their security responsibilities when escorting or handcarrying classified information. The latter requirement

may be satisfied by a briefing or by requiring the courier to read written instructions that contain the information listed below, as a minimum:

a. The courier is liable and responsible for the information being escorted;

b. The information is not, under any circumstances, to be left unattended;

c. During overnight stops, classified information is to be stored at a U.S. embassy, military or appropriately cleared DoD contractor facility (see paragraph 9-11.4d) and shall not, under any circumstances, be stored in vehicles, hotel rooms or safes;

d. The information shall not be opened enroute except in the circumstances described in subparagraph 9-11.5h;

e. The information shall not be discussed or disclosed in any public place or conveyance;

f. The courier shall not deviate from the authorized travel schedule;

g. The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents) are complete, valid, and current;

h. There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights. Carry-on bags and packages may be subjected to X-raying and inspection by customs or airline/airport security officials. If there is a question about the contents of the package, the courier shall present the courier authorization to the official or to the official's supervisor, if necessary. If the official demands to see the actual contents of the package, it may be opened in his or her presence, in an area out of sight of the general public. However, under no circumstances shall classified information be disclosed. Immediately after the examination, the courier shall request that the package be resealed and signed by the official to confirm that the package was opened. Inform both the addressee and the dispatching security officer in writing of the opening of the package;

i. The courier shall carry a copy of an inventory of the contents in the sealed package and submit a copy to the courier's security office for retention;

j. Upon return, the courier shall return all classified information in a sealed package or furnish documentation signed by an authorized security official of the addressee organization for any information that is not returned;

k. Refer to reference (f) on the handcarry of classified NATO information.

6. In the event that the handcarry of classified information will also involve the disclosure of classified information to foreign nationals, the command foreign disclosure approving official shall ensure that disclosure authorization has been obtained per reference (o).

**9-12 AUTHORIZATION TO ESCORT OR HANDCARRY CLASSIFIED INFORMATION**

1. The Security Manager shall provide written authorization to all individuals escorting or handcarrying classified information. This authorization may be the DD 2501, Courier Authorization Card, or included on official travel orders, visit requests, or a courier authorization letter. Any of these four written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or handcarry classified information (except for SCI and SAP) between DoD commands per the following, except for travel aboard commercial aircraft, in which case the provisions of paragraph 9-13 also apply:

a. The individual has a recurrent need to escort or handcarry classified information;

b. The written authorization is signed by an appropriate official in the servicing security office;

c. The expiration date may not exceed 3 years from the issue date (pertains only to DD 2501);

d. Retrieve the written authorization upon an individual's transfer, termination of employment, or when authorization is no longer required;

e. When using the DD 2501, a limited number may be issued to "Bearer," on a case-by-case basis, to individuals who need to handcarry classified information for a specific event. In this

instance, Item 2 on the card shall be annotated "Indefinite". The DD 2501 is controlled to preclude unauthorized use and local reproduction is prohibited.

2. The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to handcarry classified information aboard a U.S. military aircraft.

3. See appendix B for courier card procurement information.

## 9-13 AUTHORIZATION LETTER FOR ESCORTING OR HANDCARRYING CLASSIFIED INFORMATION ABOARD COMMERCIAL PASSENGER AIRCRAFT

1. Personnel escorting or handcarrying classified information aboard commercial aircraft shall process through the airline ticketing and boarding procedures in the same manner as other passengers. Advance coordination shall be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this regulation and Federal Aviation Administration (FAA) guidance to facilitate the courier's processing through airline ticketing, screening, and boarding procedures. Local FAA field offices can often be of assistance. During this coordination, specific advice shall be sought regarding the nature of documentation that will be required. Generally, the following will meet commercial airline security requirements:

a. The individual designated as courier shall possess an identification card that includes a photograph, date of birth, height, weight, and signature. If the identification card does not contain these items they shall be included in the written authorization.

b. The courier shall handcarry the original authorization letter and sufficient copies to provide documentation to airline officials. Prepare the authorization letter on command letterhead authorizing transport of the classified information and include the following information:

(1) The full name of the individual and employing agency;

(2) Description of the personal identification the individual will present (e.g., VA Drivers License No. 1234);

(3) Description of material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee and sender;

(4) The point of departure, destination, and known transfer points;

(5) A date of issue and expiration date;

(6) The name, title, and signature of the official issuing the letter. The official shall sign each package or carton on its face;

(7) The name and a valid U.S. Government telephone number of the official designated to confirm the courier authorization letter.

2. If a return trip is necessary, the host security official at the original destination shall conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.

**9-14 ESCORT OR HANDCARRY OF CLASSIFIED INFORMATION TO THE U.S. SENATE**

1. Top Secret packages shall be handcarried to the Office of Senate Security, Room S-407, the Capitol. Other classified packages being handcarried directly to the U.S. Senate shall be by an authorized courier, to one of the following offices:

a. The Committee on Appropriations, Room SD-119, Dirksen Building;

b. The Committee on Armed Services, Room SR-228, Russell Building. This office will accept only receipted classified packages addressed to the Chairman, the Ranking Minority Member, or to individual Committee staff members. Classified packages addressed to all others shall be delivered to the office of Senate Security;

c. The Committee on Foreign Relations, Room SD-423, Dirksen Building; or

d. The Committee on Intelligence, Room SH-211, Hart Building.

2. Under no circumstances shall classified packages be delivered directly to a Senator's personal office.

3. Mail Secret and Confidential packages only by USPS registered mail, addressed to the Director, Office of Senate Security, Room S-407, The Capitol, Washington, D.C. 20510-7114.

4. Prepare the package per paragraphs 9-8 and 9-9 with the inner envelope addressed to the intended recipient (e.g., Senator, staff member, committee, subcommittee, or other Senate office). Include a multiple-copy receipt with all classified packages handcarried to the U.S. Senate.

## REFERENCES

(a) DoD 5200.33-R, *Defense Courier Service*, 7 Nov 94

(b) *National Communications Security Instruction (NCSI) 4009, Protected Distribution Systems (U)*, 30 Dec 81

(c) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(d) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(e) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

(f) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(g) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(h) OPNAVINST S5460.4C, *Control of Special Access Programs Within the Department of the Navy (U)*, 14 Aug 81 (NOTAL)

(i) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98

(j) OPNAVINST C8126.1A, *Navy Nuclear Weapon Security (U)*, 20 Dec 94 (NOTAL)

(k) SECNAVINST 5720.42E, *DON Freedom of Information Act (FOIA) Program*, 5 Jun 91

(l) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 17 Oct 79 (NOTAL)

(m) OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI)*, 11 Feb 93

(n) DoD 5200.28, *Security Requirements for Automated Information Systems (AIS)*, 21 Mar 88 (NOTAL)

(o) SECNAVINST 5510.31B, *Policy and Procedures for Control of Foreign Disclosure in the DON*, 31 Dec 92

# EXHIBIT 9A

## TRANSMISSION OR TRANSPORTATION TO FOREIGN GOVERNMENTS

1. Classified information and/or material approved for release to a foreign government shall be transferred between authorized representatives of each government in compliance with the provisions of this exhibit. Each contract, agreement, or other arrangement that involves the release of classified material as freight to foreign entities shall either contain detailed transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials and the recipient government before release. Transportation plan requirements are outlined in paragraph 9. (DoD TS-5105.21-M-3 provides guidance regarding SCI).

2. Classified information and/or material released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated, in writing, by the recipient government to sign for and assume custody and responsibility on behalf of the government (hereafter referred to as the "designated government representative"). This written designation shall contain assurances that such a person has a security clearance at the appropriate level and that the person shall assume full responsibility for the information on behalf of the foreign government. The recipient shall be required to execute a receipt regardless of the level of classification.

3. Classified material that is suitable for transfer by courier or postal service per this regulation, and that cannot be transferred directly to a foreign government's designated representative, shall be transmitted to:

a. An embassy, consulate, or other official agency of the recipient government having extra-territorial status in the U.S.; or

b. A U.S. embassy or U.S. military organization in the recipient country or in a third party country for delivery to a designated representative of the recipient government.

4. The shipment of classified material as freight via truck, rail, aircraft, or ship shall be per the following:

a. The DoD officials authorized to approve a Foreign Military Sales (FMS) transaction that involves the delivery of

U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of a proposal, consult with DoD transportation authorities (MTMC, Military Sealift Command, Air Mobility Command, or other authority, as appropriate), to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the U.S. shall use the Defense Transportation System (DTS) to deliver classified material to the recipient government. A transportation plan shall be developed by the DoD component that prepares the Letter of Offer and Acceptance (LOA) in coordination with the purchasing government. Security officials of the DoD component that prepares the LOA shall evaluate the adequacy of the transportation plan.

b. Classified shipments resulting from direct commercial sales shall comply with the same security standards that apply to FMS shipments. To develop and obtain approval of the required transportation plan, cleared DoD contractors shall consult with the purchasing government and the DSS Regional Operating Location (OPLOC) before consummation of a commercial contract that will result in the shipment of classified material.

c. Delivery of classified material to a foreign government at a point within the U.S. and its territories shall be accomplished at:

(1) An embassy, consulate, or other official agency under the control of the recipient government;

(2) The point of origin. When a designated representative of the recipient government accepts delivery of U.S. classified material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall ensure that the recipient is aware of secure means of onward movement of the material to its final destination, consistent with the approved transportation plan;

(3) A military or commercial Port of Embarkation (POE) that is a recognized point of departure from the U.S. and its territories for on-loading aboard a ship, aircraft, or other carrier. In these cases, the transportation plan shall provide for U.S.-controlled secure shipments to the CONUS transshipment point and the identification of a secure storage facility, government or commercial, at or near the POE. A DoD official authorized to transfer custody shall supervise or observe the on-loading of FMS material being transported when physical and security custody of the material has yet to be transferred

formally to the foreign recipient. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper (government or contractor); segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility designated in the transportation plan;

(4) An appropriately cleared freight forwarder facility identified by the recipient government as its designated representative. In these cases, a person identified as a designated government representative shall be present to accept delivery of the classified material and receipt for it, to include full acceptance of security responsibility.

5. Delivery outside the U.S. and its territories:

a. U.S. classified material delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the classified material may be delivered directly to the recipient government's designated representative upon arrival.

b. U.S. classified material to be delivered to the representatives of a foreign government within a third country shall be delivered to an agency or installation of the U.S. or the recipient country which has extra-territorial status or is otherwise exempt from the jurisdiction of the third country. Unless the classified material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and deliver it to the recipient government's designated representative.

6. Overseas shipments of U.S. classified material shall be made only via ships, aircraft, or other carriers that are:

a. Owned or chartered by the U.S. Government or under U.S. registry;

b. Owned or chartered by or under the registry of the recipient government; or

c. Otherwise authorized by the head of the DoD component having classification jurisdiction over the classified material involved. Overseas shipments of classified material shall be escorted, prepared for shipment, packaged, and stored aboard as prescribed elsewhere in this regulation and in DoD 5220.22-M.

7. Only freight forwarders that have been granted an appropriate FCL by the DoD or the recipient government are eligible to receive, process related security documents, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of the classified material, and is not required to perform security-related functions, need not be cleared.

8. Foreign governments may return classified material to a U.S. contractor for repair, modification, or maintenance. At the time the classified material is initially released to the foreign government, the approved methods of return shipment shall be specified in the LOA for FMS material, the security requirements section of a direct commercial sales contract, or in the original transportation plan. The contractor, upon notification of a return shipment, shall give advance notice of arrival to the applicable cognizant contracting command or the DSS and arrange for secure inland shipment within the U.S. if such shipment has not been prearranged.

9. Transportation plan requirements:

a. Preparation and coordination:

(1) FMS. U.S. classified material to be furnished to a foreign government or international organization under FMS transactions shall normally be shipped via the DTS and delivered to the foreign government within its own territory. The U.S. Government may permit other arrangements for such shipments when it determines that the recipient foreign government has its own secure facilities and means of shipment from the point of receipt to ultimate destination. In any FMS case, the DoD component having security cognizance over the classified material involved is responsible, in coordination with the foreign recipient, for developing a transportation plan. When the point of origin is a U.S. contractor facility, the contractor and DSS shall be provided a copy of the plan by the DoD component.

(2) Commercial Transactions. The contractor shall prepare a transportation plan for each commercial contract, subcontract, or other legally binding arrangement providing for the transfer of classified freight to foreign governments, to be moved by truck, rail, aircraft, or ship. The requirement for a transportation plan applies to U.S. and foreign classified contracts. The DSS will approve transportation plans that support commercial arrangements or foreign classified contracts.

(3) The transportation plan shall describe arrangements for secure shipment of the classified material from the point of origin to the ultimate destination. It shall identify recognized POEs from the U.S. and its territories for transfer to a specified ship, aircraft, or other authorized carrier. It shall identify a government or commercial secure facility in the vicinity of the POEs and debarkation that can be used for storage if transfer or onward movement cannot take place immediately. Except as described in paragraph 9a(4), a U.S. Government official authorized to transfer custody and control shall supervise the on-loading of classified material when it has yet to be officially transferred. The plan shall provide for security arrangements in the event custody cannot be transferred promptly.

(4) Upon transfer of the title to the purchasing foreign government, classified material may be delivered to a freight forwarder that is designated, in writing, by the foreign government as its representative for that shipment and is cleared to the level of the classified information to be received. The freight forwarder shall be provided a copy of the transportation plan and agree to comply.

b. The transportation plan shall, as a minimum, include:

(1) A description of the classified material to be shipped and a brief narrative describing where and under what circumstances transfer of custody will occur;

(2) Identification, by name and title, of the designated government representative (or alternate) of the recipient government or international organization who will receipt for and assume security responsibility;

(3) Identification and specific location(s) of delivery point(s) and security arrangements while located at the delivery point(s);

(4) Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their clearance;

(5) Identification of any storage or processing facilities and transfer points to be used; certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped; and a description of security arrangements while located at the facilities;

(6) Routes and, if applicable, security arrangements for overnight stops or delays enroute;

(7) Arrangements for dealing with port security and customs officials;

(8) The identification, by name or title, of couriers, escorts, or other responsible officials (e.g. captain or crew chief) to be used, including social security number, government identification, or passport number, security clearance, and details concerning their responsibilities;

(9) Description of the shipping methods to be used and the identification of the foreign or domestic carriers;

(10) Description of packaging requirements, seals, and storage during shipment;

(11) A requirement for the recipient government or international organization to examine shipping documents upon receipt in its own territory; and a requirement to notify DSS or the DoD component having security cognizance if the information has been transferred enroute to any carrier not authorized by the transportation plan;

(12) Requirement for the recipient government or international organization to inform DSS or the DoD component having security cognizance over the classified information promptly and fully of any known or suspected compromise of the classified information;

(13) Arrangements for return shipments, if necessary for repair, modification, or maintenance.

# EXHIBIT 9B

## RECORD OF RECEIPT
## (OPNAV 5511/10)

OPNAV 5511/10 (Rev 12-89)
S/N 0107-LF-008-6000

**RECORD OF RECEIPT**
(REFERENCE OPNAVINST 5510.1H)

THIS RECEIPT MUST BE SIGNED AND RETURN

| ORIGINATOR'S CODE | FILE OR SERIAL NO. | DATE OF MATERIAL | UNCLASSIFIED DESCRIPTION | COPY NO. | NO. OF ENCLS TO MAT'L RCD |
|---|---|---|---|---|---|
| N09N2 | 12345 | (Date) | Security Classification Guide | 1 | 1 |

ADDRESSEE (Activity Receiving Material)

CNO (N09N2)

REGISTERED NUMBER

SIGNATURE (Authorized Receipt)

R.W. MARSHALL

R.W. Marshall

DATE

20 OCT 98

# CHAPTER 10

# STORAGE AND DESTRUCTION

## 10-1 BASIC POLICY

1. Commanding officers shall ensure that all classified information is stored in a manner that will deter or detect access by unauthorized persons. Classified information which is not being used or not under the personal observation of cleared persons who are authorized access shall be stored per this chapter. To the extent possible, limit areas in which classified information is stored and reduce current holdings to the minimum required for mission accomplishment.

2. Weapons or sensitive items, such as money, jewels, precious metals, or narcotics shall not be stored in the same security containers used to store classified information.

3. There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction shall not be marked or posted on the security container. This does not preclude placing a mark or symbol on the security container for other purposes or applying decals or stickers required by the DCI for security containers used to store or process intelligence information.

4. Report to the CNO (N09N3) any weakness, deficiency, or vulnerability in any equipment used to safeguard classified information. Include a detailed description of how the problem was discovered and the measures taken to mitigate it, and classify per chapter 4 of this regulation, if applicable.

## 10-2 STANDARDS FOR STORAGE EQUIPMENT

The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and destruction of classified information. Reference (a) describes acquisition requirements for physical security equipment used within the DoD.

## 10-3 STORAGE REQUIREMENTS

1. Classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container, vault,

modular vault, or secure room (open storage area constructed per exhibit 10A) as follows:

a. Store Top Secret information by one of the following methods:

(1) In a GSA-approved security container with one of the following supplemental controls;

(a) The location housing the security container shall be subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the security container once every 2 hours;

(c) An Intrusion Detection System (IDS) with personnel responding to the alarm within 15 minutes of the alarm annunciation;

(d) Security-in-Depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740; or

(e) In either of the following: (1) An open storage area (secure room) or vault which is equipped with an IDS with personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-in-Depth or a 5-minute alarm response if it is not.

b. Store Secret information by one of the following methods:

(1) In the same manner prescribed for Top Secret;

(2) In a GSA-approved security container, modular vault, or vault without supplemental controls; or

(3) In either of the following: (1) Until 1 October 2002, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved security container secured with a rigid metal lock-bar and a GSA-approved padlock, or (2) An open storage area (secure room) with one of the following supplemental controls:

(a) The location housing the open storage area is subject to continuous protection by cleared guard or duty personnel;

(b) Cleared guard or duty personnel shall inspect the area once every 4 hours; or

(c) An IDS with response time within 30 minutes of alarm annunciation.

(4) Commands are encouraged to replace non-GSA-approved cabinets with GSA-approved security containers as soon as feasible prior to the mandatory replacement date of 1 October 2002. New lock-bar cabinets shall not be fabricated from either existing or new containers, nor shall any existing lock-bar container that was not previously used for the protection of classified information be put into use for that purpose.

c. Store **Confidential** information in the same manner prescribed for Top Secret or Secret **except** that supplemental controls are not required.

2. Under field conditions during military operations, the commanding officer may require or impose security measures deemed adequate to meet the storage requirements in paragraphs 10-3.1a through c, commensurate to the level of classification.

3. Reference (b) governs the requirements for storing classified ordnance items too large to store in GSA-approved containers.

4. Storage areas for bulky material containing Secret or Confidential information may have access openings secured by GSA-approved combination padlocks (Federal Specification FF-P-110 Series), or high security key-operated padlocks (MIL-P-43607). If these storage requirements cannot be met afloat or on board aircraft, Secret or Confidential information may be stored in a locked container constructed of metal or wood (such as a foot locker or cruise box) secured by a GSA-approved padlock meeting Federal Specification FF-P-110. The area in which the container is stored shall be locked when not manned by U.S. personnel and the security of the locked area checked once every 24 hours.

5. Commanding officers shall establish standard operating procedures to include screening points, in order to ensure that all incoming mail, including bulk shipments, are secured until a determination is made as to whether or not they contain classified information. Overnight storage of certain unopened mail, overnight delivery, USPS Express, first class, certified, or registered mail (all of which could contain classified information), shall be safeguarded per chapter 7, paragraphs 7-3 through 7-5 and reference (c).

## 10-4 PROCUREMENT OF NEW STORAGE EQUIPMENT

1. If new security storage equipment is needed, procure it from the GSA Federal Supply Schedule. However, prior to procuring new storage equipment, conduct a physical security survey of existing equipment and review classified records on hand. Coordinate with the records manager to determine if it is feasible to use available equipment or to retire, return, declassify, or destroy a sufficient volume of records on hand to make the needed security storage space available. Promptly report excess containers (if any) to property disposal and fulfill requirements for added equipment through property disposal when that is more cost effective.

2. Security containers conforming to Federal Specifications have a Test Certification Label on the inside of the control locking drawer. Containers manufactured after February 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer. Specifications have been developed for 8 classes of security containers (Classes 1, 2, 3, 4, 5, 6, 7, and 8.) However, only 6 classes (Classes 1, 2, 3, 4, 5, and 6) are approved for storage of classified information, and only Classes 5 and 6 are currently on the GSA schedule. The removal of approved security containers from GSA schedule does not negate the approval. Previously approved GSA containers may still be used to store classified information provided they meet the original level of integrity and have not had the Test Certification Label removed for cause.

## 10-5 REMOVAL OF SECURITY CONTAINERS

Security containers that have been used to store classified information shall be inspected by appropriately cleared personnel before removal from protected areas or before unauthorized persons are allowed access to them. The inspection shall ensure that no classified information remains within.

## 10-6 SHIPBOARD CONTAINERS AND FILING CABINETS

1. Shipboard containers shall conform to DON standards for durability, size, weight, maintainability, and safety. Non GSA-approved filing cabinets and safe lockers of various sizes and shapes are available for use. These cabinets and safe lockers are designed and constructed according to various hull type drawings and ship drawings, and are equipped with mechanical Group 1R combination locks.

2. The requirement to store Secret and Confidential information in these types of locked containers also includes implementing supplemental security measures such as continuous operations, or locking the surrounding area when not manned by U.S. personnel with the locked area checked every 24 hours.

3. New ship construction requirements shall include GSA-approved security containers and comply with the storage requirements of this regulation.

4. Mechanical locks on existing shipboard file cabinets and safe lockers do not have to be replaced with locks meeting Federal Specification FF-L-2740.

**10-7 VAULTS AND SECURE ROOMS**

1. Entrances to vaults or secure rooms shall be under visual control during duty hours to prevent entry by unauthorized personnel, or equipped with electric, mechanical, or electro-mechanical access control devices to limit access. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford by themselves the required degree of protection for classified information and shall not be used as a substitute for the locks prescribed in paragraph 10-3.

2. Periodically examine existing areas and promptly repair correctable defects. Existing approved vaults and secure rooms do not require modification to meet current standards.

3. GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information as an alternative to vault requirements as described in **exhibit 10A**.

**10-8 SPECIALIZED SECURITY CONTAINERS**

1. GSA-approved field safes and special purpose one- and two-drawer light-weight security containers are intended primarily for storage of classified information in situations where normal storage is not feasible. These containers shall be securely fastened to the structure to render them non-portable or kept under constant surveillance to prevent their theft.

2. GSA-approved map and plan file containers are available to store odd-sized classified items such as computer media, maps, and charts.

## 10-9 NON GSA-APPROVED SECURITY CONTAINERS

Immediately remove security containers manufactured by Remington Rand from service and dispose of them under accepted safety standards. Previously approved two- and four-drawer Class 5 security containers manufactured by Art Metal Products, Inc., are no longer authorized for the protection of classified information.

## 10-10 RESIDENTIAL STORAGE

1. Top Secret information may be removed from designated areas for work at home during off-duty hours only as authorized by the SECDEF, the Secretaries of the Military Departments, the Combatant Commander, and the CNO (N09N).

2. Secret and Confidential information may be removed from designated areas for work at home during off-duty hours only as authorized by the CNO (N09N), a Fleet Commander in Chief, the Commander of the Naval Space Command, the Commanders of the Naval Systems Commands, the Chief of Naval Research, the Commandant of the Marine Corps, or the Commanding General of U.S. Marine Corps Forces Atlantic or Pacific.

3. A critical operational requirement shall exist for consideration of such requests. A GSA-approved security container shall be furnished for residential storage. Additionally, Top Secret information shall be protected with an IDS or comparable supplemental controls. Written procedures shall be developed to provide for appropriate protection of the information, to include a record of the classified information that is authorized for removal.

## 10-11 REPLACEMENT OF COMBINATION LOCKS

1. Exhibit 10B is the priority list for replacing existing mechanical combination locks with locks meeting Federal Specification FF-L-2740. The mission and location of the command, the classification level and sensitivity of the information, and the overall security posture of the command determines the priority for replacement of existing combination locks. All system components and supplemental security measures including IDS, automated entry control subsystems, video assessment subsystems, and level of operations shall be evaluated

when determining the priority for replacement of security equipment. Priority 1 requires immediate replacement.

2. New purchases of combination locks shall conform to Federal Specification FF-L-2740. Existing mechanical combination locks shall not be repaired. They shall be replaced with locks meeting Federal Specification FF-L-2740.

**10-12 COMBINATIONS**

1. Only personnel who have the responsibility and possess the appropriate clearance level shall change combinations to security containers, vaults and secure rooms. Combinations shall be changed:

a. When first placed in use;

b. When an individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock;

c. When a combination has been subjected to compromise; or

d. When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

2. The combination of a container, vault, or secure room used for the storage of classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Mark any written record of the combination with the appropriate classification level.

3. Maintain a record for each security container, vault, or secure room showing the location of each, the names, home addresses, and home telephone numbers of all persons having knowledge of the combination. Use SF 700, "Security Container Information," for this purpose.

a. Place Part 1 of the completed SF 700 on an interior location in security containers, vault or secure room doors. Mark Parts 2 and 2A of the SF 700 to show the highest classification level and any special access notice applicable to the information stored within. Store Parts 2 and 2A in a security container other than the one to which it applies. If

necessary continue the listing of persons having knowledge of the combination on an attachment to Part 2.

b. If a container is found unsecured, unattended, or shows evidence of unauthorized entry attempt, notify the appropriate official.

**10-13 KEY AND PADLOCK CONTROL**

1. Commanding officers shall establish administrative procedures for the control and accountability of keys and locks whenever high security key-operated padlocks are used. The level of protection provided each key shall be equivalent to the highest classification level of information being protected by the padlock.

2. Reference (d) makes unauthorized possession of keys, keyblanks, keyways, or locks adopted by any part of the DoD for use in the protection of conventional arms, ammunition or explosives (AA&E), special weapons, and classified equipment a criminal offense punishable by fine or imprisonment up to 10 years, or both.

3. Reference (e) governs key security and lock control used to protect classified information.

4. Reference (b) governs controls and security of keys and locks used for AA&E.

**10-14 SECURING SECURITY CONTAINERS**

When securing security containers, rotate the dial of combination locks at least four complete turns in the same direction, and check each drawer. In most locks, if the dials are given only a quick twist, it is possible to open the lock merely by turning the dial back to its opening position.

**10-15 REPAIR, MAINTENANCE, AND OPERATING INSPECTIONS**

1. Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination per reference (f) or, who are continuously escorted.

a. With the exception of frames bent through application of extraordinary stress, a GSA-approved security container

manufactured prior to October 1991 (identified by a silver GSA-label with black lettering affixed to the exterior of the container) is considered restored to its original state of security integrity as follows:

(1) If all damaged or altered parts (e.g., locking drawer, drawer head, or lock) are replaced with new or cannibalized parts; or

(2) If a container has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, the replacement lock shall meet Federal Specification FF-L-2740; the drilled hole shall be repaired with a tapered case-hardened steel rod (e.g., dowel, drill bit, or bearing) with a diameter slightly larger than the hole and of such length that when driven into the hole there remains, at each end of the rod, a shallow recess not less than 1/8 inch nor more than 3/16 inch deep to permit the acceptance of substantial welds; and the rod is welded on the inside and outside surfaces. The outside of the drawer head shall be puttied, sanded, and repainted so no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts.

b. In the interest of cost efficiency, the procedures identified in paragraph 10-15a(2) shall not be used for GSA-approved security containers purchased after October 1991 (identified by a silver GSA label with red lettering affixed to the outside of the container control drawer) until it is first determined whether warranty protection still applies. To make this determination, contact the manufacturer and provide the serial number and date of manufacture of the container. If a Class 5 security container is under warranty, use the procedures described in the Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR, "Neutralizing Locked-Out Containers," to neutralize a lock-out. If a Class 6 security container is under warranty, use the procedures described in the NFESC TDS 2010-SHR, "Red Label Class 6 Security Container Opening Procedures," to neutralize a lock-out.

2. GSA-approved containers which have been drilled in a location or repaired in a manner other than described in paragraph 10-15a(2) are not considered restored to their original state of security integrity. Remove the "Test Certification Label" on the inside of the locking drawer and the "General Services Administration Approved Security Container" label on the outside of the top drawer of the container. Place a permanently marked notice to this effect on the front of the container. As a

result, these containers may be used to store only unclassified information.

3. When repair results are visible and could be mistaken for marks left in an attempt to gain unauthorized entry to the container, stamp a registration mark in the metal of the container and post a label inside the locking drawer stating the details of the repair. Use **exhibit 10C** to record the history of the security equipment to reflect the operating problems, the type of maintenance, the date repaired/inspected, the name and company of the technician, the name of the command, and the certifying official. Retain this record for the service life of the security container/vault door.

4. External modification of GSA-approved security containers to attach additional locking devices or alarms is prohibited.

**10-16 ELECTRONIC SECURITY SYSTEM (ESS)**

1. An ESS consists of one or a combination of the following subsystems:

a. IDS;

b. Closed Circuit Television (CCTV); and

c. Access Control System (ACS).

2. An IDS monitors electronic sensors designed to detect, not prevent, an attempted intrusion. Some of the major phenomena these sensors are designed to detect are movement, changes in heat sources, door openings, and sound changes. A CCTV system is designed to assess, view areas, or detect an intrusion. Some of the major components of a CCTV system are cameras, thermal images, switchers, and video motion detectors. An ACS system is designed to help control access to spaces. Major ACS components consist of card reader devices, biometrics, and hand geometry components and the computers to control them.

3. An ESS provides additional controls at vital areas as insurance against human or mechanical failure. The use of an ESS in the protective program of a command may be required because of the critical importance of a command's mission, design, layout, or location of the facility. In some instances, their use may be justified as a more economical and efficient substitute for other protective measures.

4. Commercial IDSs used on storage containers, vaults, modular vaults, and secure rooms shall be approved by the CNO (N09N3). Existing IDSs may continue to be used and do not need approval until upgraded or replaced.

5. **Exhibit 10D** provides guidance regarding IDSs and ACSs.

**10-17 DESTRUCTION OF CLASSIFIED INFORMATION**

1. Destroy classified information no longer required for operational purposes per reference (g). Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information.

2. Commanding officers should establish at least 1 day each year "clean-out" day when specific attention and effort are focused on disposition of unneeded classified and controlled unclassified information.

3. Refer to references (h) and (i) for destroying COMSEC information, reference (j) for destroying SCI, and reference (k) for destroying NATO information.

4. Refer to reference (l) for AIS storage media destruction techniques.

5. The Directorate for Information Systems Security, NSA, provides technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media and processing equipment components.

6. Obtain specifications concerning appropriate GSA-approved equipment and standards for destruction through the National Supply System (FSC Group 36, Part II).

7. Refer to **exhibit 2B** for emergency destruction guidelines.

**10-18 DESTRUCTION METHODS AND STANDARDS**

1. Various methods and equipment may be used to destroy classified information that include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

2. A cross-cut shredder shall reduce the information to shreds no greater than 3/64 inch wide by 1/2 inch long. Strip shredders purchased prior to 29 April 1988 may continue to be used; however, new purchases shall be cross-cut shredders.

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

4. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

**10-19 DESTRUCTION PROCEDURES**

1. Commanding officers shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel. Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

2. Classified information shall be controlled in a manner designed to minimize the possibility of unauthorized removal and/or access. A burn bag may be used to store classified information awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this regulation until actually destroyed.

3. A record of destruction is required for Top Secret information. The use of OPNAV 5511/12, "Classified Material Destruction Report," is no longer required. Record destruction of Top Secret and any special types of classified information (if required) by any means as long as the record includes complete identification of the information destroyed and date of destruction. The record shall be executed by two witnesses when the information is placed in a burn bag or actually destroyed. Retain Top Secret records of destruction for 5 years. Records of destruction are not required for waste products containing Top Secret information.

4. Records of destruction are not required for Secret and Confidential information except for special types of classified information (see paragraphs 7-7 and 10-17).

**10-20 DESTRUCTION OF CONTROLLED UNCLASSIFIED INFORMATION**

1. Destroy record copies of FOUO, SBU, DoD UCNI, DOE UCNI, Sensitive (Computer Security Act of 1987), and unclassified technical documents assigned Distribution Statements B through X, per reference (g). Non-record copies may be shredded or torn into pieces and placed in trash containers. Records of destruction are not required.

2. Destroy Unclassified DEA Sensitive Information and NNPI in the same manner approved for classified information.

**10-21 DISPOSITION OF CLASSIFIED INFORMATION FROM COMMANDS REMOVED FROM ACTIVE STATUS OR TURNED OVER TO FRIENDLY FOREIGN GOVERNMENTS**

1. Commanding officers shall ensure that all classified information has been removed before relinquishing security control of a ship, shore activity, or aircraft for striking, decommissioning, deactivation, or rehabilitation. Disposal shall be per reference (g) or stored at an approved facility when the status is temporary.

a. The commanding officer shall certify to the command accepting custody that a security inspection has been conducted and that all classified information has been removed. If, for some reason, all classified information has not been removed, the certification shall document the information remaining, the authority and reason therefore.

b. Where possible, conduct the security inspection jointly with the command accepting custody.

2. Commanding officers shall ensure that the release of classified information in connection with the transfer to a friendly foreign government is processed per reference (m), and that the permission of the Archivist of the U.S. is obtained before transferring records to other agencies or non-U.S. Government organizations, including foreign governments, per reference (g).

**REFERENCES**

(a) DoD Instruction 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*, 17 Feb 89 (NOTAL)

(b) OPNAVINST 5530.13B, *DON Physical Security Instruction for Conventional Arms, Ammunition and Explosives (AA&E)*, 5 Jul 94

(c) OPNAVINST 5112.5A, *Mail Handling and Delivery Procedures for Mailrooms and Postal Service Centers*, 17 Jun 87

(d) Title 18, U.S.C., Section 1386, *Crimes and Criminal Procedures*

(e) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98

(f) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(g) SECNAVINST 5212.5D, *Navy and Marine Corps Records Disposition Manual*, 22 Apr 98

(h) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(i) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

(j) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(k) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(l) NAVSO P-5239-26, *Remanence Security Guidebook*, Sep 93

(m) SECNAVINST 5510.34, *Manual for the Disclosure of DON Military Information to Foreign Governments and International Organizations*, 4 Nov 93

# EXHIBIT 10A

## VAULT AND SECURE ROOM (OPEN STORAGE AREA) CONSTRUCTION STANDARDS

### 1. VAULT

a. Floor and Walls. Eight inches of reinforced-concrete to meet current structural standards. Walls are to extend to the underside of the roof slab.

b. Roof. Monolithic reinforced-concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling shall be reinforced-concrete of a thickness to be determined by structural requirements, but not less than the floors and walls.

d. Door. Vault door and frame unit shall conform to Federal Specification AA-D-2757, Class 8 vault door, or Federal Specification AA-D-600, Class 5 vault door. Doors shall be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740.

### 2. SECURE ROOM

a. Walls, Floor, and Roof. The walls, floor, and roof construction shall be of permanent construction materials; i.e. plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling with permanent construction materials, wire mesh, or 18-gauge expanded steel screen.

b. Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.

c. Doors. The access door to the room shall be substantially constructed of wood or metal and be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740. For open storage areas approved under previous standards, the lock may be the previously approved GSA combination lock until the door has been retrofitted with a lock meeting Federal Specification FF-L-2740. When double doors are used, an astragal will be installed on the active leaf of the door. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Doors other than the access

door shall be secured from the inside (for example, by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door, or by any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized). Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

d. Windows. All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows shall be constructed from or covered with materials which provide protection from forced entry and shall be protected by an IDS, either independently or by the motion detection sensors in the space. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

e. Openings. Utility openings such as ducts and vents shall be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches shall be hardened per the Military Handbook 1013/1A.

# EXHIBIT 10B

## PRIORITY FOR REPLACEMENT

Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.

### LOCK REPLACEMENT PRIORITIES IN THE U.S. AND ITS TERRITORIES

| ITEM | TS/SAP | TS | S/SAP | S-C |
|---|---|---|---|---|
| Vault Doors | 1 | 1 | 3 | 4 |
| Containers(A)* | 3 | 4 | 4 | 4 |
| Containers(B)** | 1 | 1 | 1 | 2 |
| Crypto | 1 | 1 | 2 | 2 |

### LOCK REPLACEMENT PRIORITIES OUTSIDE THE U.S. AND ITS TERRITORIES

| ITEM | TS/SAP | TS | S/SAP | S-C |
|---|---|---|---|---|
| Vault Doors | 1 | 1 | 2 | 2 |
| Containers(A)* | 2 | 2 | 3 | 3 |
| Containers(B)** | 1 | 1 | 1 | 2 |
| Crypto | 1 | 1 | 2 | 2 |
| High Risk Areas | 1 | 1 | 1 | 1 |

*A-Located in a controlled environment where the DoD has the authority to prevent unauthorized disclosure of classified information. The U.S. Government may control or deny access to the space, post guards, require identification, challenge presence, inspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

**B-Located in an uncontrolled area without perimeter security measures.

# EXHIBIT 10C

## MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS OPTIONAL FORM 89

**MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS**

NOTE: Store this form in the security container or on the vault door.

TYPE
☐ SECURITY CONTAINER ☐ VAULT DOOR

SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Map and Plan Containers: Located on the inside face of the door.)

MANUFACTURER

GSA CLASS
☐ ONE ☐ TWO ☐ THREE ☐ FOUR ☐ FIVE ☐ SIX ☐ SEVEN

| OPERATING PROBLEM | TYPE OF MAINTENANCE | DATE REPAIRED/ INSPECTED | TECHNICIAN | | ORGANIZATION NAME |
|---|---|---|---|---|---|
| | | | NAME | ACTIVITY | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED |
|---|---|---|
| | | |

AUTHORIZED FOR LOCAL REPRODUCTION

OPTIONAL FORM 89 (9-98)

## MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS
## OPTIONAL FORM 89 (BACK)

| OPERATING PROBLEM | TYPE OF MAINTENANCE | DATE REPAIRED/ INSPECTED | TECHNICIAN | | ORGANIZATION NAME |
|---|---|---|---|---|---|
| | | | NAME | ACTIVITY | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED |
|---|---|---|
| | | |

OPTIONAL FORM 89 (9-88) BACK

# EXHIBIT 10D

## IDS AND ACCESS CONTROLS

1. **IDS.** An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE)

b. Security forces

c. Operating procedures

2. **SYSTEM FUNCTIONS**

a. IDS components operate as a system with the following four distinct phases:

(1) Detection

(2) Reporting

(3) Assessment

(4) Response

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone" at the monitor station.

(2) Reporting: The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communications scheme. The supervised signal is intended to disguise the information and protect the IDS against tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU

signals. When an alarm occurs, an annunciator generates an audible and visual alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) Assessment: The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) Response: The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

3. **THREAT, VULNERABILITY, AND ACCEPTABILITY**

a. As determined by the commanding officer, all areas that reasonably afford access to the container, or where classified data is stored should be protected by an IDS unless continually occupied. Prior to the installation of an IDS, commanding officers shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

b. Acceptability of Equipment: All IDEs must be UL-listed (or equivalent) and approved by the DoD Component or DoD contractor. Government-installed, -maintained, or -furnished systems are acceptable.

4. **TRANSMISSION AND ANNUNCIATION**

a. Transmission Line Security: When the transmission line leaves the secured area and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(1) Class I: Class I line security is achieved through the use of a data encryption system or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institute of Standards and Technology or another independent testing laboratory is required.

(2) Class II: Class II line supervision refers to systems in which the transmission is based on pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a

minimum 6-month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. Internal Cabling: The cabling between the sensors and the PCU should be dedicated to the IDE and must comply with national and local code standards.

c. Entry Control Systems: If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion alarms.

d. Maintenance Mode: When an alarm zone is placed in the maintenance mode, this condition should automatically signal to the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to 1 second per occurrence.

e. Annunciation of Shunting or Masking Condition: Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f. Alarms Indications: Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

g. Power Supplies: Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(1) Emergency Power: Emergency power shall consist of a protected independent backup power source that provides a minimum of 4-hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall be followed and results documented.

(2) Power Source and Failure Indication: An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, and the location of the failure or change.

h. Component Tamper Protection: IDE components located inside or outside the secure area shall be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection shall be provided.

5. SYSTEM REQUIREMENTS

a. Independent Equipment: When many alarmed areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

b. Access and/or Secure Switch and PCU: No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection: Secure areas that reasonably afford access to the container or where classified information is stored should be protected with motion detection sensors (e.g., ultrasonic and passive infrared). Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

d. Protection of Perimeter Doors: Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

e. Windows: All readily accessible windows (within 18 feet of ground level) shall be protected per appendix 10A.

f. IDS Requirements for Continuous Operations Facility: A continuous operations facility may not require an IDS. This type

of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

g. False and/or Nuisance Alarm: Any alarm signal transmitted in the absence of a detected intrusion or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed one in a period of 30 days per zone.

6. INSTALLATION, MAINTENANCE, AND MONITORING

a. Installation and Maintenance Personnel: Alarm installation and maintenance should be accomplished by U.S. citizens who have been subjected to a trustworthiness determination per SECNAVINST 5510.30A.

b. Monitor Station Staffing: The monitor station shall be supervised continuously by U.S citizens who have been subjected to a trustworthiness determination per SECNAVINST 5510.30A.

7. ACCESS CONTROLS. The perimeter entrance should be under visual control at all times during working hours to prevent entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard CCTV). Regardless of the method used, an ACS shall be used on the entrance. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures at the facility.

a. Automated Entry Control Systems (AECS): An automated entry control system may be used to control admittance during working hours instead of visual control, if it meets the AECS criteria stated in subparagraphs 7.a and b below. The AECS must identify an individual and authenticate the person's authority to enter the area through the use of an identification badge or card.

(1) Identification Badges or Key Cards. The identification badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification: Personal identity verification (Biometrics Devices) identifies the individual requesting access by some unique personal characteristic, such as:

(a) Fingerprinting

(b) Hand Geometry

(c) Handwriting

(d) Retina scans

(e) Voice recognition

A biometrics device may be required for access to the most sensitive information.

b. In conjunction with subparagraph 7.a(1) above, a personal identification number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

c. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the identification badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

d. Protection must be established and maintained for all devices or equipment which constitute the entry control system. The level of protection may vary depending upon the type of device or equipment being protected.

(1) Location where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

(2) Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall

have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(3) Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(4) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

(5) Electric strikes used in access control systems shall be heavy duty, industrial grade.

e. Access to records and information concerning encoded identification data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

f. Records shall be maintained reflecting active assignment of identification badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved, and recorded.

g. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need-to-know and access. The Heads of DoD components may approve the use of standardized AECS which meet the following criteria:

(1) For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

(2) For a Level 2 key card and PIN system, the AECS must provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

(3) For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a 0.97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made.

h. Electric, Mechanical, or Electromechanical Access Control Devices: Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following manner:

(1) The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel (located within the area) will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

(3) The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest level of classified information controlled within.

(4) Electrical components, wiring included, or mechanical links (cables, rods, etc.) should be accessible only from inside the area, or, if they traverse an uncontrolled area they should be secured within protecting covering to preclude surreptitious manipulation of components.

# CHAPTER 11

# INDUSTRIAL SECURITY PROGRAM

## 11-1 BASIC POLICY

1. Commanding officers shall establish an industrial security program if their commands engage in classified procurement or when cleared DoD contractors operate within areas under their direct control. Command security procedures shall include appropriate guidance, consistent with this regulation, to ensure that classified information released to industry is safeguarded.

2. Commanding officers responsible for the acquisition of classified defense systems shall comply with the requirements of reference (a), which establishes policy and assigns responsibilities for identifying and protecting classified information or controlled unclassified information that has been identified as critical to the combat effectiveness of systems being developed within the DON acquisition programs.

3. Commanding officers responsible for the acquisition of classified defense systems shall develop a Program Protection Plan (PPP) to fulfill the requirements of reference (a). Because contractor facilities are included, cleared DoD contractors may assist in developing the PPP for a classified contract. Requirements levied on contractors in the PPP shall be conveyed in the contract document itself or on the DD 254 (see **exhibit 11A**).

## 11-2 AUTHORITY

1. Reference (b) established the NISP for safeguarding information released to industry classified under reference (c), or its successor or predecessor orders, and reference (d). This regulation implements the requirements of the NISP within the DON. Provisions of this regulation relevant to operations of cleared DoD contractor employees entrusted with classified information shall be applied by contract or other legally binding instrument.

2. Reference (e) imposes the requirements, restrictions, and safeguards necessary to prevent unauthorized disclosure of classified information released by U.S. Government executive branch departments and agencies to their contractors.

3. Reference (f) imposes requirements, restrictions, and safeguards necessary to protect special classes of information

beyond those established in the baseline portion of reference (e).

## 11-3 DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY MISSION

1. **The Chief Operating Officer for DSS** oversees DoD implementation of the NISP through 12 OPLOCs throughout the CONUS. An additional OPLOC will be established to oversee the international aspects of the NISP (formerly known as Office of Industrial Security International). OPLOCs provide administrative assistance and policy guidance to local DSS field elements charged with security oversight of cleared DoD contractors located in CONUS that perform on classified contracts. Consult the DSS Homepage at http://www.dis.mil for information pertaining to various DSS functions.

2. **DSS, Operations Center Columbus (OCC)** grants personnel clearances to individuals in private industry who require access to classified information in order to perform their jobs. The OCC also grants FCLs within the NISP, refers cases with major adverse information to the Defense Office of Hearings and Appeals for adjudication, processes overseas visit requests, and responds to requests for information regarding personnel clearances and FCL applications, and facility storage capability.

## 11-4 CLEARANCE UNDER THE NISP

An employee of a contractor granted an FCL under the NISP may be processed for a personnel clearance when the contractor determines that access is essential in the performance of tasks or services related to a classified contract or an IR&D program (see chapter 8, paragraph 8-8 of reference (g) for contractor-granted clearances, Interim Secret and Confidential personnel clearances, Limited Access Authorizations (LAAs), and adverse information reporting).

## 11-5 DSS AND COMMAND SECURITY OVERSIGHT OF CLEARED DoD CONTRACTOR OPERATIONS

1. **Shipboard.** On board ship, cleared DoD contractor employees have visitor status and shall conform to the requirements of this and command security regulations. Cleared DoD contractors shall submit written requests to the commanding officer who will then grant approval for classified visits by employees to the ship.

2. **Shore Installations.** Commanding officers shall establish or coordinate security oversight over classified work carried out by cleared DoD contractor employees in spaces controlled or occupied

at DON shore installations. Command oversight shall be carried out by exercising one of the following options:

a. The commanding officer requests, in writing, that the DSS OCC grant the contractor an FCL and that DSS assume security oversight.

b. The commanding officer requests, in writing, that the DSS OCC grant the contractor an FCL with the command retaining security oversight. Commands shall conduct periodic reviews and forward a copy of the Industrial Security Inspection Report to the DSS OPLOC which exercises geographic jurisdiction over the installation. Contractors granted an FCL under these first two options assume the status of a tenant activity.

c. The commanding officer determines that the contractor is a short- or long-term visitor and decides that an FCL is not warranted. Contractor employees shall conform with command security regulations and shall be included in the command security education program.

3. **Off-Site Locations.** When contractors perform work at locations other than the command awarding the contract, the awarding command shall inform the new host. Forward to the host command a copy of the notification of contract award, a copy of the DD 254, and other pertinent documents.

4. **DON Overseas Locations.** Commands that award classified contracts requiring performance by cleared DoD contractors at DON overseas locations shall ensure that this regulation is enforced in all aspects of contract security administration.

a. DSS provides administrative assistance to both U.S. Government and industry overseas, maintains PCL data on all cleared DoD contractor employees assigned overseas, provides security education, and conducts oversight of contractor operations at U.S. Government-controlled and U.S. military overseas installations.

b. Contractors located overseas are not granted FCLs; therefore, the cognizant DSS OPLOC will normally exercise security oversight over all contractor operations located at DON overseas locations and coordinate with the cognizant command prior to conducting assist visits or reviews.

c. Commanding officers who wish to exercise security oversight authority over cleared contractors at their commands shall request approval from the DSS.

d. Contracting commands awarding a classified contract for which the DSS is relieved of responsibility in whole or in part for contractor performance at overseas locations shall coordinate as necessary with the host command to ensure the DSS OPLOC representatives are given proper guidance when fulfilling their responsibilities.

## 11-6 FACILITY ACCESS DETERMINATION (FAD) PROGRAM

The Internal Security Act of 1950 entrusts commanding officers to protect persons and property against the actions of untrustworthy persons. This regulation confirms the FAD program within the DON to assist commands in making trustworthiness determinations on contractor employees for access eligibility to controlled unclassified information or sensitive areas and equipment under DON control. Trustworthiness determinations pertain to unclassified contracts for various services (e.g., janitorial, guards, equipment maintenance). Commands shall take the necessary steps to include the conditions of the FAD program in the specifications of all contracts needing trustworthiness determinations, thereby eliminating the necessity to award a classified contract for performing services only. Reference (g) addresses specific requirements for administering the FAD program.

## 11-7 CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)

Commanding officers shall ensure that a DD 254 is incorporated into each classified contract. The DD 254, with its attachments, supplements, and incorporated references, is designed to provide a contractor with the security requirements and classification guidance needed for performance on a classified contract. An original DD 254 shall be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly. A revised DD 254 shall be issued as necessary during the lifetime of the contract when security requirements change. A final DD 254 shall be issued on final delivery or on termination of a classified contract (see exhibit 11A for a sample DD 254).

## 11-8 COR INDUSTRIAL SECURITY RESPONSIBILITIES

1. Paragraph 2-6 identifies the appointment of a qualified security specialist as a COR.

2. The following industrial security responsibilities are normally assigned to the COR, but are not limited to the following:

a. Review statement of work to ensure that access to or receipt and generation of classified information is required for contract performance.

b. Validate security classification guidance, complete, and sign the DD 254:

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

(2) Issue a revised DD 254 and other guidance as necessary.

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

c. Provide when necessary, in coordination with the program manager, additional security requirements, beyond those required by this regulation, in the DD 254, or the contract document itself.

d. Initiate all requests for FCL action with the DSS OCC.

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

f. Validate justification for Interim Top Secret PCLs and FCLs.

g. Validate and endorse requests submitted by industry for LAAs for non-U.S. citizen employees of cleared contractors.

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

i. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions or issue a final DD 254.

j. Certify and approve Registration For Scientific and Technical Information Services requests (DD 1540).

k. Review reports of security violations and compromises within industry and forward to program managers.

l. Ensure that timely notice of contract award is given to host commands when contractor performance is required at other locations.

**11-9 CONTRACTOR BADGES**

Echelon 2 commands shall establish administrative procedures governing the expiration date and retrieval of contractor badges.

**11-10 VISITS BY CLEARED DoD CONTRACTOR EMPLOYEES**

Cleared contractors shall furnish advance notification to the commanding officer of the DON command being visited. In urgent cases, visit information may be furnished by telephone, provided it is promptly confirmed in writing. Commands shall not accept a visit request handcarried by a cleared DoD contractor. The responsibility for determining the need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Final approval of a visit is the prerogative of the commanding officer of the visited command. Reference (g) addresses visit requirements for cleared DoD contractor employees.

**11-11 CONTRACTOR FACILITY CLEARANCES**

1. If a cleared contractor's FCL needs to be upgraded or revalidated, the cognizant contracting command shall submit a written request to the DSS OCC. Contractors, when eligible, are automatically granted Interim Secret or Confidential FCLs during processing of a final FCL when requested by a U.S. Government or industry sponsor. However, as an emergency measure and in order to avoid crucial delays in contract negotiations, award or performance, Interim Top Secret FCLs may be granted on a temporary basis, pending completion of full investigative requirements.

2. DON contracting commands requiring an Interim Top Secret FCL for a contractor facility shall submit a request, in writing, to the DSS OCC. The request shall be validated by the COR and endorsed by the commanding officer or designee. Unless otherwise limited by security concerns, the request shall clearly identify the contractor by name, location, commercial and government entity code, current level of FCL, include a copy of the completed DD 254 for the contract or program, and, indicate the effect that any crucial delays will have on contract

negotiations, award, or performance. Every effort shall be made to provide sufficient information to properly fulfill the request. The DSS OCC will take appropriate action and will notify the requesting command when action is completed.

**11-12 TRANSMISSION OR TRANSPORTATION**

1. Appropriately cleared and designated DoD contractor employees may act as couriers, escorts, or handcarriers provided that:

a. They have been briefed by their facility security officer on their responsibility to safeguard classified information;

b. They possess an identification card or badge, which contains their name, photograph, and the company name;

c. Employees retain classified information in their personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability, and

d. The transmission or transportation meets all other requirements specified in chapter 9.

2. Appropriately cleared DoD contractors may use the GSA commercial contract carrier for overnight delivery of Secret and Confidential information to U.S. Government agencies within CONUS when procedures have been formally approved by the DSS OPLOC prior to starting such transmissions (see reference (h)).

**11-13 DISCLOSURE**

1. Disclose classified information only to contractors cleared under the NISP. Prior to disclosing classified information, the custodian shall determine that the contractor requires access in connection with a legitimate U.S. Government requirement (e.g., contract solicitation, precontract negotiation, contractual relationship, or IR&D effort).

2. Determinations shall be based on the following:

a. An FCL valid for access at the same or lower classification level as the FCL granted, and

b. Storage capability.

3. The DSS OCC Central Verification Activity (CVA) or contractor's OPLOC provides written verification of the FCL level and storage capability within 5 working days after receipt of the command's inquiry. Each verification remains valid for a period of 3 years from date of issuance. The OCC CVA provides any changes that adversely affect the security classification level of the FCL or storage capability to the requesting command. Inquiries shall be made by letter, facsimile, or telephone. Contact the CVA via e-mail at discofac@dislink.jcte.jcs.mil or telephonically (1-888-282-7682) for verifications involving the storage of 2 cubic feet, or less, of classified information. Contractor storage capability involving the storage of over 2 cubic feet shall be verified directly with the cleared contractor.

4. When classified contracts are awarded for performance at DON commands overseas, the following additional security measures shall be taken prior to disclosing classified information to cleared DoD contractors:

a. Verify that the requirement for access to classified information overseas is essential to the fulfillment of the classified contract.

b. Require that classified information provided to cleared DoD contractors performing overseas is stored at a U.S. Government-controlled facility or military installation unless a written waiver or exception to this requirement is granted by the CNO (N09N2).

c. Furnish the overseas installation commander and the responsible DSS OPLOC with a notice of contract award, any special instructions (e.g., transmission, storage, and disposition instructions), and a copy of the original DD 254.

d. Transmission or transportation of classified information to U.S. Government locations overseas shall comply with the requirements of chapter 9.

5. Obtain an assurance of a foreign contractor employee's clearance level and need-to-know prior to allowing access to U.S. classified information authorized for use in joint contracts with NATO activities or foreign governments under agreement with the U.S. The DSS OPLOC will verify the security clearance and status of foreign contractor employees.

6. Privately-owned or proprietary information, including information relating to trade secrets, processes, operations,

materials, style of work or apparatus, statistics relating to costs or income, profits or losses shall not be published or disclosed without the express written permission of, and in strict accordance with, any conditions stated by the legal owner or proprietor of the information.

7. Restrictions on the release of information previously imposed by a competent authority govern in each case.

8. A system exists within DoD to certify individuals and enterprises qualified to receive export-controlled technical data. These individuals and enterprises are referred to as Qualified Contractors. This certification is accomplished using a Militarily Critical Technical Data Agreement, DD 2345 (Jul 95).

9. Upon receipt of a request for export-controlled technical data with military or space application, a command shall determine if:

a. The requestor is a Qualified Contractor verified by an approved DD 2345 from the U.S./Canada Joint Certification Office, Defense Logistics Service Center, Federal Center, 74 N. Washington, Battle Creek, MI 49017-3084.

b. Certification under the Joint Certification Program establishes the eligibility of a U.S. or Canadian contractor to receive technical data governed by reference (i).

**11-14 *RELEASE OF* INTELLIGENCE TO CLEARED DoD CONTRACTORS**

1. Appropriately cleared and access-approved DoD contractors may receive intelligence information in support of a DON classified contract (e.g., authorized on the DD 254) without prior approval of the Director, ONI (ONI-5) who is responsible for executing the policy and procedures governing the release of intelligence to cleared DoD contractors and is the final appeal authority on release denials.

2. Prior to releasing intelligence to a cleared DoD contractor, the releasing command shall:

a. Ensure that dissemination is not prohibited by paragraph 11-16.

b. Ensure that the conditions of paragraph 11-17 are met.

c. Ensure that all intelligence released falls within the scope of the contract under which requested. When any part of a

document is released, the releasing command shall sanitize the intelligence.

3. The releasing command shall maintain a record of all intelligence released to contractors and report releases to the originator upon request.

4. Program managers and CORs shall ensure that the following requirements are included in the contract itself or in the DD 254:

a. Intelligence released to cleared DoD contractors, all reproductions thereof, and all other information generated based on, or incorporating data from, remain the property of the U.S. Government. The releasing command shall govern final disposition of intelligence information unless retention is authorized. Provide the Director, ONI (ONI-5) with a copy of the retention authorization.

b. Cleared DoD contractors shall not release intelligence to any of their components or employees not directly engaged in providing services under contract or other binding agreement or to another contractor (including subcontractors) without the consent of the releasing command.

c. Cleared DoD contractors who employ foreign nationals or immigrant aliens shall obtain approval from the Director, ONI (ONI-5) before releasing intelligence, regardless of their LAA.

5. National Intelligence Estimates, Special National Intelligence Estimates, and Interagency Intelligence Memoranda may be released to appropriately cleared DoD contractors with the requisite need-to-know except as governed by provisions concerning proprietary information.

**11-15 PROHIBITED RELEASE OF INTELLIGENCE**

1. Obtain the consent of the originator via the Director, ONI (ONI-5) prior to releasing intelligence to a cleared DoD contractor which:

a. Bears either of the following control markings:

(1) CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN) (see chapter 6, paragraph 6-12);

(2) DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON) (see chapter 6, paragraph 6-12);

b. Originates from Foreign Service reporting; or

c. Is marked for special handling in specific dissemination channels.

2. Address requests for authority to release the above intelligence information to the Director, ONI (ONI-5), via the command sponsoring the contract for validation of need-to-know, and include the following information:

a. Cleared DoD contractor's name for whom the intelligence is intended;

b. Contract number supporting the request;

c. Cognizant contracting command's name;

d. Certification of contractor's FCL and storage capability;

e. Complete identification of the information for which a release determination is desired; and

f. Justification confirming need-to-know and a concise description of that portion of the contractor's study or project which will confirm the need-to-know for the requested intelligence information. This statement is a prerequisite for a release determination.

**11-16 SANITIZATION OF INTELLIGENCE**

1. Any command releasing intelligence to a cleared DoD contractor is responsible for proper sanitization. If the releasing command is not aware of specific contractual commitments, coordinate release of the intelligence with those activities which are able to determine the scope of the contract and need-to-know requirements of the contractor.

2. Delete any reference to the CIA phrase "Directorate of Operations," the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to release that information is obtained from CIA. Forward any requests for approval via the Director, ONI (ONI-5).

## REFERENCES

(a) DoD Directive 5200.1-M, *Acquisition System Protection Program*, 16 Mar 94 (NOTAL)

(b) Executive Order 12829, *National Industrial Security Program*, 6 Jan 93

(c) Executive Order 12958, *Classified National Security Information*, 17 Apr 95

(d) Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act* of 30 Aug 54, as amended

(e) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(f) DoD 5220.22-M.Supp 1, *National Industrial Security Program Operating Manual Supplement 1, (NISPOMSUP)* Feb 95 (NOTAL)

(g) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(h) ISL 97-1, *Industrial Security Letter*, Jul 97

(i) OPNAVINST 5510.161, *Withholding of Unclassified Technical Data from Public Disclosure*, 29 Jul 85

# CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)

**DEPARTMENT OF DEFENSE**
**CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

*(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)*

**1. CLEARANCE AND SAFEGUARDING**
a. FACILITY CLEARANCE REQUIRED
b. LEVEL OF SAFEGUARDING REQUIRED

**2. THIS SPECIFICATION IS FOR:** (X and complete as applicable)
a. PRIME CONTRACT NUMBER
b. SUBCONTRACT NUMBER
c. SOLICITATION OR OTHER NUMBER — Due Date (YYMMDD)

**3. THIS SPECIFICATION IS:** (X and complete as applicable)
a. ORIGINAL (Complete date in all cases) — Date (YYMMDD)
b. REVISED (Supersedes all previous specs) — Revision No. — Date (YYMMDD)
c. FINAL (Complete item 5 in all cases) — Date (YYMMDD)

**4. IS THIS A FOLLOW-ON CONTRACT?** [ ] YES [ ] NO. If Yes, complete the following:
Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.

**5. IS THIS A FINAL DD FORM 254?** [ ] YES [ ] NO. If Yes, complete the following:
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____

**6. CONTRACTOR** (Include Commercial and Government Entity (CAGE) Code)
a. NAME, ADDRESS, AND ZIP CODE: Enter the prime contractor here
b. CAGE CODE
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code): To facilitate distribution use the servicing DSS operating location

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

**8. ACTUAL PERFORMANCE**
a. LOCATION: Enter other "contractor" locations
b. CAGE CODE
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

**9. GENERAL IDENTIFICATION OF THIS PROCUREMENT**

Enter a short, consise, and unclassified description of the procurement action here.

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

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

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

[ ] Direct [ ] Through (Specify):

Complete this item to direct the contractor to the office within your command responsible for reviewing proposed public releases.

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

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

This is the most important part of the DD 254. Use this item to identify applicable guides, to provide narrative guidance which identifies the specific types of information to be classified, to provide downgrading or declassification instructions, to provide any special instructions, explanations, comments or statements required for information or to clarify any other items on the DD 254. Each contract is unique in its performance requirements. Write the guidance in plain english. It's *not necessary to put all the guidance in this space.* Use additional pages as needed to expand or explain guidance.

The DD 254, with its attachments is the only authorized means for providing classification guidance to a contractor. It should be written as specifically as possible and include only that information that pertains to the contract for which it is issued. It should not contain references to internal DON directives or instructions unless such documents provide instructions applicable to the contract. If so, the pertinent portions should be extracted and provided as attachments. All documents referenced or cited in item 13 should be furnished to the contractor, either as attachments or under separate cover if they are classified. *Requirements of the NISPOM should not be cited.* The NISPOM provides safeguarding requirements for classified information not security classification guidance. Security classification guidance provides detailed information regarding what information requires classification, at what level, and assigns downgrading or declassification instructions that apply to the information or material generated by the contractor in performance of the contract. Retention and disposition instructions for classified information should be reviewed and updated throughout the life of the contract.

Encourage the contractor to assist in the preparation of the classified guidance and provide comments or recommendations for changes in the guidance when necessary. Effective communication with the contractor will result in understandable classification guidance that will ensure the appropriate classification and protection of the information generated by the contractor.

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

YES in this item signifies that security requirements over and above those of the baseline NISPOM will be imposed. The contracting command is required to incorporate the additional requirements into the contract document itself or in item 13. Costs due to additional security requirements can be reimbursable to the contractor.

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

YES in this item relieves DSS of inspection authority for the contract and requires that specific information on "carved out" areas and inspection cognizance be furnished to the contractor.

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

| a. TYPED NAME OF CERTIFYING OFFICIAL | b. TITLE | c. TELEPHONE (Include Area Code) |
|---|---|---|
| B. Gobel | Contracting Officer's Representative | COM (202) 433-8860<br>DSN 288-8860 |

| d. ADDRESS (Include Zip Code) | 17. REQUIRED DISTRIBUTION |
|---|---|
| Chief of Naval Operations (N09N2)<br>Washington Navy Yard, Building 111<br>Washington, DC 20388-5381 | [ ] a. CONTRACTOR<br>[ ] b. SUBCONTRACTOR<br>[ ] c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR<br>[ ] d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION<br>[ ] e. ADMINISTRATIVE CONTRACTING OFFICER<br>[ ] f. OTHERS AS NECESSARY |
| e. SIGNATURE<br>B. Gobel | |

DD Form 254 Reverse, DEC 90

# CHAPTER 12

# LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

## 12-1 BASIC POLICY

1. The loss or compromise of classified information presents a threat to the national security. Reports of loss or compromise ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of the loss or compromise and to preclude recurrence.

2. A loss of classified information occurs when it cannot be physically located or accounted for.

3. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access or a need-to-know.

4. A possible compromise occurs when classified information is not properly controlled.

## 12-2 REPORTING RESPONSIBILITIES

1. **Individual.** An individual who becomes aware that classified information is lost or compromised shall immediately notify their commanding officer or security manager of the incident. If that individual believes their commanding officer or security manager may be involved in the incident, notify the next higher echelon of command or supervision. If circumstances of discovery make such notification impractical, the individual shall notify the commanding officer or security manager at the most readily available command or contact the local NCIS office.

2. **Commanding Officer.** When a loss or compromise of classified information occurs, the cognizant commanding officer shall immediately notify the local NCIS office and initiate a Preliminary Inquiry (PI). The contacted NCIS office shall promptly advise whether or not they will open an investigation and provide advice. Timely referral to the NCIS is imperative to ensure preservation of evidence for any possible CI or criminal investigation.

## 12-3 PRELIMINARY INQUIRY (PI)

A PI is the initial process to determine the facts surrounding a possible loss or compromise. At the conclusion of the PI, a narrative of the PI findings are provided in support of recommended additional investigative or command actions. A PI is convened by the command with custodial responsibility over the lost or compromised information.

## 12-4 PRELIMINARY INQUIRY INITIATION

1. The commanding officer shall appoint, in writing, a command official (other than the security manager or anyone involved with the incident) to conduct a PI.

2. A PI shall be initiated and completed within 72 hours and sent by message or letter to the next superior in the administrative chain of command, the CNO (N09N2), the originator and the OCA of the lost or compromised information, the local NCIS office, and all others required by paragraph 12-8. If circumstances exist that would delay the completion of the PI within 72 hours, all the required addressees shall be notified. A pending NCIS investigation shall not delay the completion of a PI, unless the NCIS Special Agent in Charge (SAC) requests that command actions be held in abeyance in order to preserve evidence for CI or criminal investigations.

## 12-5 CONTENTS OF THE PI MESSAGE OR LETTER

The PI shall completely and accurately identify the information lost or compromised. This identification shall include the information's subject or title, classification of the information (including any relevant warning notices or intelligence control markings, downgrading and declassification instructions), all identification or serial numbers, the date, the originator, the OCA, the number of pages or amount of material involved, a point of contact from the command, a command telephone number, the Unit Identification Code (UIC) of the custodial command, etc. (see exhibits 12A and 12B for sample PI formats).

## 12-6 CLASSIFICATION OF THE PI MESSAGE OR LETTER

Every effort shall be made to keep the PI unclassified and without any enclosures. However, if the lost information is beyond the jurisdiction of the U.S., and cannot be recovered, the PI shall be classified commensurate to the security classification level of the lost information to prevent its recovery by unauthorized persons.

## 12-7 ACTIONS TAKEN UPON PI CONCLUSION

1. Send the PI message or letter if the PI concludes that a loss or compromise of classified information occurred or a significant command security weakness(es) or vulnerability(ies) is revealed. The command shall immediately initiate a JAGMAN investigation (see paragraphs 12-9 and 12-10), and notify the local NCIS office and all required addressees of the PI. Additionally, the commanding officer shall immediately take any necessary disciplinary and/or corrective actions to prevent further damage and recurrence.

2. Send the PI message or letter if the PI concludes that a loss or compromise of classified information may have occurred. Additionally, the command shall initiate a JAGMAN investigation (see paragraph 12-9 and 12-10) and immediately notify the local NCIS office and all required addressees of the PI. If a significant security weakness or vulnerability is revealed due to the failure of a person(s) to comply with established security practices and/or procedures the commanding officer shall immediately take any necessary disciplinary and/or corrective actions to prevent recurrence.

3. Do not send the PI message or letter if the PI concludes that a loss or compromise of classified information did not occur or the possibility of compromise is remote (e.g., "remote" due to security-in-depth at the command). However, if a minor security weakness or vulnerability is revealed due to the failure of a person(s) to comply with established security practices and/or procedures, the commanding officer shall immediately take the necessary disciplinary and/or corrective actions to prevent recurrence.

## 12-8 REPORTING LOSSES OR COMPROMISES OF SPECIAL TYPES OF CLASSIFIED INFORMATION AND EQUIPMENT

1. Report losses or compromises involving computer systems, terminals, or equipment to the CNO (N09N2) (the CNO (N09N2) shall notify the Director, Information Assurance, OASD($C^3I$)).

2. Report losses or compromises involving NATO classified information per reference (a). One of the primary requirements of reference (a) is to notify the USSAN via the ODUSD(PS). This notification shall be made by the CNO (N09N2).

3. Report losses or compromises involving FGI to the CNO (N09N2) (the CNO (N09N2) shall notify the Director, International Security Programs (ODUSD(PS)).

4. Report losses or compromises involving **DoD SAPs**, or results of inquiries or investigations that indicate weaknesses or vulnerabilities in established SAP policy, to the Director, Special Programs (ODUSD(PS)) via CNO (N89).

5. Report losses or compromises involving **Restricted Data** (including **CNWDI**), and **Formerly Restricted Data** (when it involves unauthorized disclosure to a foreign government), to the CNO (N09N2) with a copy to the local NCIS office, who shall notify the FBI.

6. Report losses or compromises involving **SIOP and SIOP-ESI** to the Joint Chiefs of Staff (JCS) and the U.S. Commander in Chief, Strategic Command (USCINCSTRAT) by the quickest means possible, consistent with security requirements. Include an opinion as to the probability of compromise. The USCINCSTRAT will then recommend appropriate actions with regard to modification of the plan or related procedures for consideration by the JCS.

7. Report losses or compromises of **COMSEC** information or keying material to the controlling authority, who shall determine if a traffic review is necessary. If a review is warranted, it shall be conducted using the procedures contained in reference (b). The "initial report" required by reference (b) satisfies the requirement for a PI (see paragraph 12-2), provided copies are sent to the CNO (N09N2), the NSA, and the local NCIS office. Aside from this one exception, the procedures set forth in reference (b) shall be followed in addition to, and not in lieu of, the requirements of this chapter.

8. Report losses or compromises involving **SCI** per reference (c).

9. Report losses or compromises of classified information which involve other Government agencies to the Principal Director, Security and Information Operations (ODASD(S&IO)). It is the Principal Director, Security and Information Operations (ODASD(S&IO)) who is notified in those instances when other U.S. government agencies lose or compromise DoD classified information.

10. Immediately report incidents indicating a deliberate compromise of classified information or indicating possible involvement of a **foreign intelligence agency** to the local NCIS office.

## 12-9 JAGMAN INVESTIGATIONS

1. A JAGMAN investigation is an administrative proceeding conducted per chapter II of reference (d). A JAGMAN investigation is usually convened by the command having custodial responsibility over the information lost or compromised. The purpose of a JAGMAN investigation is to provide a more detailed investigation and recommend any corrective or required disciplinary actions.

2. Whenever serious disciplinary action or prosecution is contemplated against any person(s) believed responsible for the compromise of classified information, formal classification reviews (see paragraph 12-16) shall be coordinated with the CNO (N09N2), the NCIS and the OJAG (Code 11). Whenever a violation of criminal law appears to have occurred and criminal prosecution is contemplated, the OJAG (Code 11) shall notify the DON General Counsel.

3. Designation as a national security case (see reference (d)) does not normally occur until the JAGMAN investigation is completed and it has been submitted to the appointing authority (cognizant command).

## 12-10 JAGMAN INITIATION AND APPOINTMENT LETTER

1. The commanding officer shall appoint, in writing, an individual to conduct a JAGMAN investigation. This individual shall have a clearance level commensurate to the classification level of the information involved; the ability to conduct an effective investigation; and shall **not** be someone likely to have been involved, directly or indirectly, with the incident. The command security manager shall **not** be appointed to conduct the JAGMAN investigation (see **exhibit 12C** for a sample JAGMAN appointment letter).

2. If during the course of the JAGMAN investigation it is determined that a compromise did not occur, the investigation shall be terminated and all addressees required in paragraphs 12-3 and 12-8) shall be notified with a brief statement supporting the determination.

3. **Exhibit 12D** is a sample format for a JAGMAN investigation. Questions concerning JAGMAN investigations shall be directed to the cognizant DON command's Staff Judge Advocate (SJA) or the nearest Trial Service Office.

## 12-11 INVESTIGATIVE ASSISTANCE

Successful completion of a JAGMAN investigation may, under certain circumstances, require professional or technical assistance. Commanding officers may ask the NCIS for investigative assistance in cases where commands lack either the resources or the capabilities to conduct certain types of investigations. Such a request may be made at any time during the course of the investigation, regardless of whether the NCIS initially declined investigative action. For example, the NCIS can provide valuable assistance in interviewing witnesses who have been transferred or in processing latent fingerprints.

## 12-12 CLASSIFICATION OF JAGMAN INVESTIGATIONS

1. Every effort shall be made to keep the JAGMAN investigation unclassified; however, it shall be classified under the same circumstances as a PI (see paragraph 12-6).

2. An NCIS Report of Investigation (ROI) shall not be made part of a JAGMAN investigation. The NCIS ROIs are exempt from certain disclosure provisions of reference (e), while JAGMAN investigations are not. By attaching the NCIS ROI to the JAGMAN investigation, the attached NCIS ROI loses its exempt status and may be disclosed in total under reference (e). Extracts or statements acquired through the NCIS ROI may be used in findings of fact, but that use shall first be approved by the originating NCIS office. Particular attention shall be given to the handling instructions on the NCIS ROI cover sheet provided to commands and instructions contained in paragraph 0217H(2) of reference (d).

## 12-13 RESULTS OF JAGMAN INVESTIGATIONS

Upon completion of the JAGMAN investigation, the convening command shall forward the investigation via the administrative chain of command with letters of endorsement, to the CNO (N09N2). Information copies shall be forwarded to the local NCIS office, the originator and the OCA, unless the originator or the OCA is assigned to the office of the CNO or a command outside the DoD, in which case the CNO (N09N2) shall forward the results of the investigation.

## 12-14 REVIEW AND ENDORSEMENT OF JAGMAN INVESTIGATIONS BY SUPERIORS

1. Each superior in the administrative chain of command shall review JAGMAN investigations for completeness and return any deficient JAGMAN investigation for additional investigation or

corrective actions. Additionally, each superior shall, by endorsement:

a. Approve or disapprove the proceedings, findings of fact, opinions, and recommendations.

b. State and evaluate the corrective measures taken, directed, or recommended to prevent recurrence of the incident. Remedial action(s) to prevent similar incidents is very important and shall be specifically addressed.

c. Determine whether security practices are in conflict with this regulation and if they are being corrected;

d. State and review the disciplinary action(s) taken or recommended to ensure it is appropriate and commensurate to the circumstances and culpability. If disciplinary action is not taken because of extenuating or mitigating circumstances explain why. Affirm that the command shall comply with reference (f), concerning continuing evaluation of the responsible individual's eligibility for clearance and access.

**12-15 SECURITY REVIEWS**

Classified information subjected to compromise requires a security review for classification determination. If local expertise is available, a security review shall be conducted for a classification determination. If no such expertise is available, the originator or OCA of the information may be asked for a security review. A security review, however, is usually insufficient to support formal prosecution. A local reviewer, shall not declassify properly classified information, unless they are the cognizant OCA.

**12-16 CLASSIFICATION REVIEWS**

1. When it is determined that a compromise of classified information has occurred, the NCIS may request the CNO (N09N2) to initiate a classification review. The CNO (N09N2) shall then coordinate a classification review of the compromised information with the cognizant OCA.

2. Upon notification by the CNO (N09N2), the cognizant OCA shall conduct a classification review of the compromised information. The classification review shall include:

a. Verification of the current security classification level and its duration.

b. The security classification level of the information when subjected to compromise.

c. Whether further review is required by some other DON command.

d. A general description of the impact on the affected operations.

3. Based on the results of this evaluation, the OCA shall select one of the following courses of action:

a. Continue classification without changing the information involved;

b. Modify specific information, in whole or part, to minimize or nullify the effects of the compromise while retaining the classification level;

c. Upgrade the information;

d. Downgrade the information; or

e. Declassify the information.

4. Upon completion of the classification review, the OCA shall evaluate the course of action chosen and notify the CNO (N09N2) of the results. If the course of action is to modify, upgrade, downgrade or declassify information, the OCA is to notify all holders of the changed information, unless the information exists in a DON SCG in which case the OCA shall submit a SCG change per reference (g).

**12-17 DAMAGE ASSESSMENTS**

1. Per reference (h), a damage assessment is a multi-disciplinary analysis to determine the effect of a compromise of classified information on the national security. It is normally a long-term, post-prosecutorial effort to determine in great detail the practical effects of an espionage-related compromise on operations, systems, materials, and intelligence. The formal damage assessment is not to be confused with the brief impact statement on the harm to national security included by the OCA in a classification review performed in support of a prosecution. Depending upon the circumstances of the compromise, a formal damage assessment is not always necessary.

2. The Department of Defense Damage Assessment Committee (DODDAC) is the committee established to review and analyze damage assessments of compromised U.S. classified defense information that result from espionage. The CNO (N09N) and the CMC (CIC) are permanent members of the DODDAC.

**12-18 PUBLIC MEDIA COMPROMISES**

1. A public media compromise is the unofficial release of DoD classified and unclassified information to the public resulting in its unauthorized disclosure.

2. When an individual or command becomes aware that classified or unclassified information is unofficially released to the public (i.e., newspaper, magazine, book, pamphlet, radio, television broadcast or INTERNET) they shall immediately notify the CNO (N09N2) (see paragraph 12-8 for additional reporting requirements for special types of information). DON personnel shall not, under any circumstances, make any statements or comments concerning any information unofficially released to the public.

3. The CNO (N09N2) is responsible for ensuring that all known or suspected instances of unauthorized public disclosure of classified information are promptly reported, investigated, and appropriate corrective action(s) is taken. Upon notification of a compromise through the public media, the CNO (N09N2) shall consult with the Office of Information (CHINFO), the Assistant SECDEF(PA), the NCIS, other officials having primary interest in the information, and:

a. Determine whether the information has been officially released (under proper authority) and, if not, obtain a classification review from the cognizant OCA;

b. Recommend any appropriate investigative action(s) to the NCIS;

c. If the information is, or appears to be, under the cognizance of another DoD component, forward the case to the DASD(S&IO), who shall determine investigative responsibility; and

d. Follow-up and keep records on any actions involving unauthorized disclosure of classified information. If no action is taken, that fact shall be recorded.

4. The NCIS shall:

a. Promptly initiate an investigation(s), if warranted. Prepare summaries of the investigation(s) and forward them to the DASD(S&IO);

b. Provide assistance to the DASD(S&IO), other DoD components, or the FBI in cases involving unauthorized public disclosure of DON information; and

c. Follow up and keep records on unauthorized public disclosure cases. If no action(s) is taken, that fact shall be recorded.

## 12-19 SECURITY DISCREPANCIES INVOLVING IMPROPER TRANSMISSIONS

Any command that receives classified information improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the command determines that the classified information has been subjected to compromise, the receiving command shall immediately notify the forwarding command. Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent where the contents are exposed, or it has been transmitted over unprotected communication circuits (e.g. facsimile, telephone, teletype, data links). If the command determines that the information was not subjected to compromise, but improperly prepared or transmitted, the receiving command shall report the discrepancy to the forwarding command, using OPNAV 5511/51 (Security Discrepancy Notice, **exhibit 12E**)). Retain Security Discrepancy Notices for 2 years.

## REFERENCES

(a) OPNAVINST C5510.101D, *NATO Security Procedures*, 17 Aug 82 (NOTAL)

(b) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)* 25 Feb 98 (NOTAL)

(c) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(d) JAGINST 5800.7C, *Manual of the Judge Advocate General*, 3 Oct 90 (NOTAL)

(e) Title 5 of Public Law 93-579, *The Privacy Act*, (U.S.C., Section 552a)

(f) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(g) OPNAVINST 5513.1E, *DON Security Classification Guides*, 16 Oct 95

(h) DoD Instruction 5240.11, *Damage Assessments*, 23 Dec 91

**EXHIBIT 12A**

**SAMPLE PI LETTER FORMAT**

5500
Ser
(Date)

From: (Title, name, grade/rank, command of investigating official)
To: (Addressee)
Via: (If any)

Subj: PRELIMINARY INQUIRY (PI)

Ref: (a) SECNAVINST 5510.36
(b) (If any)

Encl: (1) (If any)

1. **INCIDENT:** Per reference (a), (State specifics of the incident, e.g., "On (date) a PI was conducted into the possible loss or compromise of classified information at (command). A (TS, S, or C) document(s) was determined missing during a command inspection by Sgt. Smith at 1400....").

2. **STATEMENT OF FACTS:**

a. **IDENTIFICATION OF INFORMATION OR EQUIPMENT LOST OR COMPROMISED:**

(1) **CLASSIFICATION:** (Include warning notices/intelligence control markings).

(2) **IDENTIFICATION/SERIAL NO(S):**

(3) **DATE:**

(4) **ORIGINATOR:**

(5) **OCA(S):**

(6) **SUBJECT OR TITLE:**

(7) **DOWNGRADING/DECLASSIFICATION INSTRUCTIONS:**

(8) **NUMBER OF PAGES OR ITEMS OF EQUIPMENT INVOLVED:**

Subj: PRELIMINARY INQUIRY (PI)

(9) **COMMAND POINT OF CONTACT AND PHONE NUMBER:**

(10) **UIC OF CUSTODIAL COMMAND:**

b. **ASSESSMENT OF LIKELIHOOD OF LOSS OR COMPROMISE:** (Provide supporting information in either instance. Indicate if a security review of the information was conducted, and state recommendations, if any, of actions needed to be taken to minimize the effects of damage).

c. **NOTIFICATION OF LOCAL NCIS OFFICE:** (Identify the NCIS Office and SA notified. Indicate if the NCIS accepted or declined the investigation).

d. **CIRCUMSTANCES SURROUNDING THE INCIDENT:** (Provide explanation of contributing factors and include any interviews with witnesses).

e. **INDIVIDUAL(S) RESPONSIBLE:** (If any).

f. **PUNITIVE DISCIPLINARY ACTION(S) TAKEN:** (If any).

g. **DETERMINATION OF SECURITY WEAKNESS(ES) OR VULNERABILITY(IES):** (State any command weakness(es) or vulnerability(ies) that may have contributed to the incident).

3. **CONCLUSION:** (Choose one of following statements):

a. A loss or compromise of classified information did not occur, but incident meets the criteria of a security discrepancy;

b. A loss or compromise of classified information did not occur, however, a security weakness(es) or vulnerability(ies) is revealed due to the failure of a person(s) to comply with established security regulations;

c. A loss or compromise of classified information may have occurred but the probability of compromise is remote and the threat to the national security minimal;

d. A loss or compromise of classified information may have occurred due to a significant command security weakness(es) or vulnerability(ies); or

Subj: PRELIMINARY INQUIRY (PI)

e. A loss or compromise of classified information occurred, and the probability of damage to the national security cannot be discounted until after completion of a JAGMAN or NCIS investigation;

4. **CORRECTIVE MEASURES TAKEN AS A RESULT OF THE INCIDENT:** (If any).

5. **FURTHER ACTION:** (Indicate either that "No further action is required" or "A JAGMAN investigation has been initiated").

//S//

Copy to:
CNO (N09N2)
NCIS
ORIGINATOR
OCA(s)
(All others required)

## EXHIBIT 12B

## SAMPLE PI MESSAGE FORMAT

ROUTINE
R (DTG)
FM CG SECOND MAW//G-2//
TO COMMARFORLANT/G-2//
INFO CMC WASHINGTON DC//CIC//
CNO WASHINGTON DC//N09N2//
NAVCRIMINVSERVRA CHERRY PT NC

UNCLASS //N05500//
SUBJ/PRELIMINARY INQUIRY (PI)
REF/A/INST/SECNAVINST 5510.36//
RMKS/1. IAW REF A, THE FOLLOWING PI IS SUBMITTED:
A. INCIDENT: (STATE SPECIFICS OF THE INCIDENT, E.G., ON (DATE) A PI WAS CONDUCTED INTO THE POSSIBLE LOSS OR COMPROMISE OF CLASSIFIED INFORMATION AT (COMMAND). A (TS, S, OR C) DOCUMENT(S) WAS DETERMINED TO BE MISSING DURING A COMMAND INSPECTION BY SGT. SMITH AT 1400....).
B. STATEMENT OF FACTS: (IDENTIFICATION OF INFORMATION OR EQUIPMENT LOST OR COMPROMISED).
1. CLASSIFICATION: (INCLUDE WARNING NOTICES/INTELLIGENCE CONTROL MARKINGS).
2. IDENTIFICATION/SERIAL NO(S):
3. DATE:
4. ORIGINATOR:
5. OCA(S):
6. SUBJECT OR TITLE:
7. DOWNGRADING/DECLASSIFICATION INSTRUCTIONS:
8. NUMBER OF PAGES OR ITEMS OF EQUIPMENT INVOLVED:
9. COMMAND POC AND PHONE NUMBER:
10. UIC OF CUSTODIAL COMMAND:
C. ASSESSMENT OF LIKELIHOOD OF LOSS OR COMPROMISE: (PROVIDE SUPPORTING INFORMATION IN EITHER INSTANCE. INDICATE IF A SECURITY REVIEW OF THE INFORMATION WAS CONDUCTED, AND STATE RECOMMENDATIONS, IF ANY, OF ACTIONS NEEDED TO BE TAKEN TO MINIMIZE THE EFFECTS OF DAMAGE).
D. NOTIFICATION TO THE LOCAL NCIS OFFICE: (PROVIDE THE IDENTITY OF THE NCIS OFFICE AND SA NOTIFIED. INDICATE IF NCIS ACCEPTED OR DECLINED THE INVESTIGATION).
E. CIRCUMSTANCES SURROUNDING THE INCIDENT: (PROVIDE EXPLANATION OF CONTRIBUTING FACTORS AND INCLUDE ANY INTERVIEWS WITH WITNESSES).
F. INDIVIDUAL(S) RESPONSIBLE: (IF ANY).
G. PUNITIVE DISCIPLINARY ACTION(S) TAKEN: (IF ANY).

SUBJ: PRELIMINARY INQUIRY (PI)

H. DETERMINATION OF SECURITY WEAKNESS(ES) OR VULNERABILITY(IES): (STATE, IF ANY, COMMAND WEAKNESS(ES) THAT MAY HAVE CONTRIBUTED TO THIS INCIDENT).

I. CONCLUSION: (CHOOSE ONE OF THE FOLLOWING STATEMENTS: (1) A LOSS OR COMPROMISE OF CLASSIFIED INFORMATION DID NOT OCCUR, BUT INCIDENT MEETS THE CRITERIA OF A SECURITY DISCREPANCY; (2) A LOSS OF COMPROMISE OF CLASSIFIED INFORMATION DID NOT OCCUR, HOWEVER, A SECURITY WEAKNESS(ES) OR VULNERABILITY(IES) IS REVEALED DUE TO THE FAILURE OF A PERSON(S) TO COMPLY WITH ESTABLISHED SECURITY REGULATIONS; (3) A LOSS OR COMPROMISE OF CLASSIFIED INFORMATION MAY HAVE OCCURRED BUT THE PROBABILITY OF COMPROMISE IS REMOTE AND THE THREAT TO THE NATIONAL SECURITY MINIMAL; (4) A LOSS OR COMPROMISE MAY HAVE OCCURRED DUE TO A SIGNIFICANT COMMAND SECURITY WEAKNESS(ES) OR VULNERABILITY(IES); OR (5) A LOSS OR COMPROMISE OF CLASSIFIED INFORMATION OCCURRED, AND THE PROBABILITY OF DAMAGE TO THE NATIONAL SECURITY CANNOT BE DISCOUNTED UNTIL AFTER COMPLETION OF A JAGMAN OR NCIS INVESTIGATION.

J. CORRECTIVE MEASURES TAKEN AS A RESULT OF THE INCIDENT: (IF ANY).

K. FURTHER ACTION: (INDICATE EITHER THE "NO FURTHER ACTION IS REQUIRED" OR "A JAGMAN INVESTIGATION HAS BEEN INITIATED").

## EXHIBIT 12C

## SAMPLE JAGMAN APPOINTMENT LETTER

5830
Ser
(Date)

From: Commanding Officer, Headquarters Battalion, Marine Corps Base, Camp Pendleton, CA
To: CAPT James E. Smith, USMC

Subj: INVESTIGATION OF THE LOSS OR COMPROMISE OF CLASSIFIED INFORMATION THAT OCCURRED AT (COMMAND) ON (DATE)

Ref: (a) JAG Manual

1. Under Chapter II, part A, of reference (a), you are appointed to investigate, as soon as practical into circumstances surrounding the loss or compromise of classified information that occurred at (command) on (date).

2. You are to investigate all the facts, circumstances, and the cause of the loss or compromise and provide identification of all compromised information and any potential impact on the national security. You should recommend appropriate administrative or disciplinary action(s). Particular attention should be given to reference (a).

3. Report your findings of fact, opinions, and recommendations by (date), unless an extension of time is granted.

4. By copy of this appointing order, Commanding Officer, Headquarters Company, is directed to furnish necessary reporters and clerical assistance for recording the proceedings and preparing the record.

//S//

Copy to:
(if any)

# EXHIBIT 12D

## SAMPLE JAGMAN INVESTIGATION FORMAT

5830
Ser
(Date)

From: (Name, title, grade/rank, command of investigating official)
To: (Addressee)

Subj: JAGMAN INVESTIGATION FORMAT

Ref: (a) SECNAVINST 5510.36
(b) (JAGMAN appointment ltr)
(c) (JAGINST 5800.7C of 3 Oct 1990)
(d) (Any others)

Encl: (1) (If any)

1. **TYPE OF INCIDENT:** (Loss or compromise).

2. **IDENTIFICATION OF LOST OR COMPROMISED INFORMATION OR EQUIPMENT:**

a. **CLASSIFICATION:** (Include warning notices/intelligence control markings).

b. **IDENTIFICATION/SERIAL NO(S):**

c. **DATE:**

d. **ORIGINATOR:**

e. **OCA(S):**

f. **SUBJECT OR TITLE:**

g. **DOWNGRADING/DECLASSIFICATION INSTRUCTIONS:**

h. **NUMBER OF PAGES OR ITEMS OF EQUIPMENT INVOLVED:**

i. **COMMAND POINT OF CONTACT AND PHONE NUMBER:**

j. **UIC OF CUSTODIAL COMMAND:**

Subj: JAGMAN INVESTIGATION FORMAT

3. **NOTIFICATION OF OCA AND LOCAL NCIS OFFICE:** (Affirm that the OCA, local NCIS office and cognizant command were notified in a timely manner, and that the NCIS took immediate action upon notification (i.e., action initiated, declined jurisdiction)).

4. **INTERVIEWS:** (Interview all involved parties. Coordinate with the NCIS or the JAG agents to avoid interviewing a criminal suspect or "designated party." Include the following information):

a. **NAME/GRADE OR RANK/BILLET TITLE:** (Do not use SSNs unless absolutely necessary for positive identification).

b. **TESTIMONY(IES):**

5. **WHEN:** (Period of time during which the information was lost or compromise).

6. **WHERE:** (Location) (If controlled space, identify all those who had access to the space, and identify all geographic ports of call, airfields or ocean areas involved, if warranted). **NOTE: WHEN CLASSIFIED INFORMATION OR EQUIPMENT IS LOST IN FOREIGN COUNTRIES AND CANNOT BE RECOVERED, THE LOCATION (this paragraph and the entire JAGMAN investigation) SHALL BE CLASSIFIED AT THE SAME LEVEL AS THE LOST INFORMATION OR EQUIPMENT.**

7. **HOW:** (The loss or compromise occurred, and how this determination was derived).

8. **INDIVIDUAL(S) RESPONSIBLE:** (If culpability is indicated).

a. **NAME:** (In full).
b. **DPOB:** (City and state).

9. **SECURITY REVIEW:** (State if information or equipment is classified properly, and on what authority you base your findings. Provide any supporting data for your conclusions(s). **DO NOT CONFUSE THIS WITH A "FORMAL CLASSIFICATION REVIEW" THAT REQUIRES FORMAL TASKING BY THE CNO (N09N2) AND REQUIRED FOR ALL NATIONAL SECURITY CASES INVOLVING A COURT-MARTIAL OR FEDERAL CRIMINAL TRIAL).**

10. **FINDINGS OF FACTS:** (Chronology of the circumstances surrounding the incident. Facts should be substantiated by witness statements or precise identification of paragraphs in other enclosures of the investigation).

Subj: JAGMAN INVESTIGATION FORMAT

**NOTE: IF INFORMATION WAS DISCLOSED VERBALLY, OR IF THE CLASSIFICATION WAS IN QUESTION, REFERENCE THE CLASSIFICATION SOURCE OR SCG(S), OR AN OPINION (LOCAL SUBJECT MATTER EXPERT) TO SUPPORT YOUR FINDINGS.**

11. **SUMMARY OF EVENTS THAT LED TO COMPROMISE:** (Based on your facts of findings, and interviews with individual involved).

12. **PROBABILITY OF COMPROMISE:** (Based on your investigation, state your opinion as to the probability of compromise (e.g., the likelihood that a loss or temporarily loss (uncontrolled information), or an unauthorized disclosure actually resulted in compromise). If you disagree with the PI findings say so. If you are certain that neither a loss or compromise occurred, and that no serious security weakness(es), vulnerability(ies) or punitive disciplinary action(s) are warranted, you may, with the convening command's approval, provide written notification to all PI addressees and end your investigation.

13. **RECOMMENDATION OF CORRECTIVE ACTION(S):** (State any corrective actions necessary to prevent recurrence).

14. **RECOMMENDATION OF PROPOSED DISCIPLINARY ACTION(S):** (If required by appointing letter, recommend any proposed disciplinary action(s)).

//S//

Copy to:
CNO (N09N2)
ORIGINATOR
OCA(s)
NCIS
(All others required)

# EXHIBIT 12E

## SECURITY DISCREPANCY NOTICE

SECURITY DISCREPANCY NOTICE

OPNAV 5511/51 (3-80) S/N 0107-LF-055-5359 (This form replaces OPNAV 5511/8; 22 AND 24 which are obsolete)

| FROM | DATE |
|---|---|
| | |

REF a. _____ (Insert ref. (s)) b. SECNAVINST 5510.36

D-CC.

TO: ⌐ ¬

(Note - This form may be in a window)

L ⌋

1. Reference (a) has been found to be inconsistent with or in contravention of reference (b) for the reason(s) checked below.
2. If applicable, corrective action should be taken and where this involves changing classification, all holders of reference (a) should be notified accordingly.

| IMPROPER TRANSMITTAL/PACKAGING | | | | | |
|---|---|---|---|---|---|
| | SENT VIA NON-REGISTERED/ NON-CERTIFIED MAIL | | CLASSIFICATION NOT MARKED ON INNER CONTAINER | | RECEIVED IN POOR CONDITION; COMPROMISE IMPROBABLE |
| | SENT IN SINGLE CONTAINER | | NO RETURN RECEIPT | | ADDRESSED IMPROPERLY |
| | MARKINGS ON OUTER CONTAINER DIVULGE CLASSIF. OF CONTENTS | | INADEQUATE WRAPPING, NOT SECURELY WRAPPED OR PROTECTED | | OTHER (Specify) |
| **CLASSIFICATION** | | | | | |
| | BASIC CLASSIFICATION QUESTIONABLE | | DOCUMENT SUBJECT MARKING | | CHART, MAP OR DRAWING MARKING |
| | OVERALL MARKINGS | | DOCUMENT TRANSMITTAL MARKING | | PHOTO, FILM OR RECORDING MARKING |
| | PARAGRAPH/COMPONENT MARKINGS | | MESSAGE MARKING | | OTHER (Specify) |
| **DOWNGRADING/DECLASSIFICATION** | | | | | |
| | CLASSIFICATION AUTHORITY NOT IDENTIFIED OR AUTHORIZED | | DOWN GRADING DATA INCORRECT | | DECLASSIFICATION DATA OMITTED OR INCORRECT |

OTHER (Specify)

Fold here 1 with face of form on top

COMMENTS (Continue on reverse, if necessary)

| SIGNATURE | TITLE |
|---|---|
| | |

# APPENDIX A

## DEFINITIONS AND ABBREVIATIONS

**Access** - The ability and opportunity to obtain knowledge or possession of classified information.

**Agency** - Any "Executive agency," as defined in 5 U.S.C., 105; any "Military Department" as defined in 5 U.S.C. 102; and any other entity within the Executive Branch that comes into the possession of classified information. The DON is an agency but each DON command is not; rather, a command is part of an agency, the DON. Within the DoD, the Departments of the Army, Navy, and Air Force are agencies.

**Assist Visit** - The informal assessment of the security posture of a command to be used as a self-help tool.

**Associated Markings** - The classification authority, office of origin, warning notices, intelligence and other special control markings, and declassification/downgrading instructions of a classified document.

**Automatic Declassification** - The declassification of information based upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum time for duration of classification established under E.O. 12958.

**Automated Information System (AIS)** - An assembly of computer hardware, software, or firmware configured to collect, create, compute, communicate, disseminate, process, store, or control data or information.

**Carve-Out** - A classified contract issued in connection with an approved SAP in which the DSS has been relieved of inspection responsibility in whole or in part under the NISP.

**Classification** - The determination by an authorized official that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure.

**Classification Authority** - The authority by which information is classified (see OCA).

**Classification Guide** - See Security Classification Guide.

**Classification Management** - The management of the life cycle of classified information from its inception to its eventual declassification or destruction.

**Classified Contract** - Any contract that requires or will require access to classified information by a contractor or its employees in the performance of the contract.

**Classified National Security Information (or "Classified Information")** - Information that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of E.O. 12958 or any predecessor Order.

**Classified Material** - Any matter, document, product or substance on or in which classified information is recorded or embodied.

**Classifier** - An approved official who makes a classification determination and applies security classification to information. A classifier may be an approved OCA, designated in **exhibit 4A**, or a derivative classifier who assigns a security classification based on a properly classified source or classification guide.

**Cleared Contractor** - Any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government and granted an FCL by the CSA for the purpose of performing on a classified contract, license, IR&D program, or other arrangement that requires access to classified information.

**Cleared DoD Contractor Employee** - As a general rule, this term encompasses all contractor employees granted a personnel security clearance under the NISP. The requirements prescribed for a cleared contractor employee should be interpreted to include, as appropriate, company officers, consultants, employees issued an LAA, and employees possessing contractor-granted Confidential clearances.

**Code Word** - A single classified word assigned a classified meaning by an appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified Confidential or higher.

**Cognizant Security Agency** - Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

**Cognizant Security Office (CSO)** - See Operating Location (OPLOC).

**Collateral Information** - Information identified as NSI under the provisions of E.O. 12958 but which is not subject to enhanced security protection required for SAP or other compartmented information.

**Command** - For the purpose of this regulation, any organizational entity under one official authorized to exercise direction and control. The term includes, base, station, unit, laboratory, installation, facility, activity, detachment, squadron, and ship.

**Commanding Officer** - For the purpose of this regulation, the head of any DON organizational entity. The term includes commander, commanding general, director, and officer in charge, and any other title assigned to an official, military or civilian, who, through command status, position or administrative jurisdiction, has the authority to render a decision with regard to a specific question under consideration.

**Communications Security (COMSEC)** - The protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. COMSEC includes: (1) Cryptosecurity, which results from providing technically sound cryptosystems and their proper use; (2) Physical security, which results from physical measures taken to safeguard COMSEC material; (3) Transmission security, which results from measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis; and (4) Emission security, which results from measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of compromising emanations from cryptoequipment and telecommunications system.

**Compromise** - An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.

**Confidential Source** - Any individual or organization that has provided, or may provide, information to the U.S. on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

**Consignee** - A person, firm, or government named as the receiver of a shipment; one to whom a shipment is consigned.

**Consignor** - A person, firm or government activity by whom articles are shipped. The consignor is usually the shipper.

**Constant Surveillance Service (CSS)** - A transportation protective service provided by a commercial carrier qualified by the MTMC to transport Confidential shipments.

**Continental United States (CONUS)** - United States territory, including adjacent territorial waters, located within the North America continent between Canada and Mexico.

**Contracting Command** - A DON command with procurement authority to award contracts to industry.

**Contracting Officer** - A Government official, who, per the departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representatives of the contracting officer, acting within the limits of their authority.

**Contracting Officer's Representative (COR)** - A security specialist at a DON contracting command who has been appointed a COR and delegated authority on behalf of the command for the security administration of classified contracts. The COR serves as the responsible official for any problems or questions related to security requirements and/or classification guidance for classified contracts (formerly known as Contracting Officers Security Representative).

**Controlled Cryptographic Item** - A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled.

**Controlled Unclassified Information** - Official information not classified or protected under E.O. 12958 or its predecessor orders that requires the application of controls and protective measures for a variety of reasons.

**Counterintelligence (CI)** - Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine activities, sabotage, international terrorist activities, or assassinations.

**Critical Nuclear Weapons Design Information (CNWDI)** - Top Secret or Secret RD revealing the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, and high explosive material by type. Among these excluded items are the components which personnel set, maintain, operate, test, or replace.

**Critical Technology** - Technology that consists of: (1) Arrays of design and manufacturing know-how (including technical data); (2) keystone manufacturing, inspection, and test equipment; (3) keystone materials; and (4) 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 U.S. (also referred to as militarily critical technology).

**Cryptanalysis** - The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption.

**Cryptography** - The branch of cryptology that treats the principles, means, and methods of designing and using cryptosystems.

**Cryptology** - The branch of knowledge that treats the principles of cryptography and cryptanalysis; and the activities involved in SIGINT and maintaining COMSEC.

**Custodial Responsibility** - The command which has classified information, or is charged with responsibility for its safeguarding, at the time of its loss or compromise.

**Custodian or Custodial Command** - The individual or command who has possession of, or is otherwise charged with the responsibility for safeguarding classified information.

**Damage to the National Security** - Harm to the national defense or foreign relations of the U.S. resulting from the unauthorized disclosure of classified information.

**Declassification** - The determination by an authorized official that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure.

**Declassification Authority** - The official who authorizes original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority, in writing, by the agency head or the senior agency official.

**Deliberate Compromise** - Any intentional act of conveying classified information to any person not officially authorized to receive it.

**Derivative Classification** - The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and ensuring that it continues to be classified by marking or similar means when included in newly created material.

**Disclosure** - Conveying classified information to another person.

**Document** - Any physical medium such as any publication (bound or unbound printed material such as reports, studies, manuals), correspondence (such as military and business letters and memoranda), electronic media, audio-visual material (slides, transparencies, films), or other printed or written products (such as charts, maps) on which information is recorded or stored.

**DoD Component** - The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense agencies.

**Downgrading** - The determination by an approved authority that information classified at a specific level requires a lower degree of protection, therefore, reducing the classification to a lower level.

**Event** - An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification or downgrading of information.

**Exception** - A written, CNO (N09N2)-approved long-term (36 months or longer) or permanent deviation from a specific safeguarding requirement of this regulation. Exceptions require compensatory security measures.

**Facility Security Clearance (FCL)** - An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

**File Series** - Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

**Foreign Government** - Any national governing body organized and existing under the laws of any country other than the U.S. and its possessions and trust territories and any agent or instrumentality of that government.

**Foreign Government Information (FGI)** - Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; information produced by the U.S. under or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or information received and treated as FGI under the terms of a predecessor order to E.O. 12958.

**Foreign Intelligence** - The product from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the U.S. and which is provided by a Government agency that is assigned an intelligence mission.

**Foreign National** - Any person not a U.S. citizen, U.S. national, or immigrant alien. American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for purposes of this regulation, when acting in that capacity.

**Foreign Recipient** - A foreign government or international organization, to whom the U.S. is providing classified information.

**Formerly Restricted Data (FRD)** - Information removed from the DOE RD category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as RD.

**Government-to-Government** - Transfers by Government officials through official channels or through other channels specified by the governments involved.

**Industrial Security** - That portion of information security which is concerned with the protection of classified information entrusted to U.S. industry.

**Information** - Any official knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

**Information Security** - The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

**Information Systems Security (INFOSEC)** - The protection of information systems against unauthorized access to or the modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

**Information Systems Security Manager (ISSM)** - A person responsible for developing, maintaining, and directing the implementation of the INFOSEC program within the command. The ISSM advises the commanding officer on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program (Previously the ADP systems security officer (ADPSSO)).

**Information Systems Security Officer (ISSO)** - A person(s) responsible for implementing and maintaining the command's information system and network security requirements.

**Infraction** - Any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that does not comprise a "violation."

**Inspection** - An official examination of the security posture of a command to determine compliance with ISP policy.

**Intelligence** - The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

**Intelligence Activity** - An activity that an agency within the intelligence community is authorized to conduct under E.O. 12333.

**Intelligence Community** - U.S. organizations and activities identified by E.O. 12333 as making up the Community. The following organizations currently comprise the Intelligence Community: CIA; NSA; DIA; special offices within the DoD for the collection of specialized foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the DOS; the intelligence elements of the military services, FBI, DEA, Departments of Treasury and Energy and the DEA; and staff elements of the Office of the DCI.

**Interim Top Secret Facility Clearance** - Clearance granted by DSS/OCC following authorization by a U.S. Government activity to avoid crucial delays in precontract or contract negotiations, the award of a contract, or performance on a contract.

**Inventory** - The process of accounting for classified information.

**Interagency Security Classification Appeals Panel (ISCAP)** - A panel that will (1) decide on appeals by persons who have filed classification challenges; (2) approve, deny, or amend agency exemptions for automatic declassification; and (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review.

**Judge Advocate General (JAG) Manual Investigation** - A proceeding conducted per chapter II of the Manual of the Judge Advocate General. It is usually ordered by the command having custodial responsibility for the classified information which has been compromised or subjected to compromise.

**Mandatory Declassification Review** - Review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of E.O. 12958.

**Marking** - The physical act of indicating on classified material the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on the use of the classified information.

**Multiple Sources** - Two or more source documents, classification guides, or a combination of both.

**National Industrial Security Program (NISP)** - National program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government and serves as a single, integrated, cohesive industrial security program to protect classified information and preserve U.S. economic and technological interests.

**National Security** - The national defense or foreign relations of the U.S.

**National Security Information (NSI)** - Any official information that has been determined under E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is so designated. The designations Top Secret, Secret, and Confidential are used to identify such information and are usually referred to as "classified information."

**Naval Nuclear Propulsion Information (NNPI)** - All information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and naval nuclear power plant prototypes, including the associated nuclear support facilities.

**Need-to-know** - A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Governmental function.

**Network** - A system of two or more computers that can exchange data or information.

**Nickname** - A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

**Official Information** - Information which is owned by, produced for or by, or is subject to the control of the U.S. Government.

**Operating Location (OPLOC)** - A DSS office that provides administrative assistance and policy guidance to local DSS field elements charged with security oversight of cleared DoD contractors performing on classified contracts.

**Original Classification** - An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

**Original Classification Authority (OCA)** - An official authorized in writing, either by the President, an agency head, or other official designated by the President "to classify information originally" or "to make an original classification decision."

**Permanent Historical Value** - Those records that have been identified in an agency's records schedule as being permanently-valuable.

**Possessions** - U.S. possessions are the U.S. Virgin Islands, Guam, American Samoa, Swain's Island, Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern Island), Kingman Reef, Johnston Atoll, Navassa Island, Swan Island, Wake Island, and Palmyra Island.

**Preliminary Inquiry (PI)** - The "initial" process to determine the facts surrounding a possible loss or compromise. A narrative of the PI findings are required when there is a loss or compromise of classified information.

**Program Manager** - Senior level official responsible for managing all aspects of development, production, and delivery related to an acquisition program. Develops program strategies and identifies industry roles and requirements in support of their programs.

**Program Review** - Formal assessment of the security posture of a command to be used in improving the management of the ISP.

**Protective Security Service (PSS)** - A transportation protective service provided by a cleared commercial carrier qualified by the MTMC to transport Secret material.

**Qualified Contractor** - A private individual or enterprise located in the U.S. or Canada whose eligibility to obtain unclassified export controlled technical data has been established following certification of an Export-Controlled DoD and Canada Technical Data Agreement, DD 2345.

**Record** - All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any command of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that command or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the information value of data in them.

**Regrade** - To raise or lower the classification assigned to an item of information.

**Report of Investigation (ROI)** - Official report of investigation conducted by agents of the NCIS.

**Restricted Data (RD)** - All data concerning: (1) Design, manufacture, or utilization of atomic weapons; (2) The production of special nuclear material; or (3) The use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category under Section 142 of the AEA, as amended.

**Risk Management** - The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

**Safeguarding** - Measures and controls prescribed to protect classified information.

**Security Classification Guide (SCG)** - The primary reference source for derivative classifiers to identify the level and duration of classification for specific informational elements. DON OCAs are required to prepare an SCG for each system, plan, program or project under their cognizance which creates classified information.

**Security-In-Depth** - A determination by the commanding officer that a command's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the command. Examples include perimeter fences, employee and visitor access controls, use of IDSs, random guard patrols during non-working hours, closed circuit video monitoring, and other safeguards that reduce the vulnerability of unalarmed storage areas and security storage cabinets.

**Self-Inspection** - The internal review and evaluation of a command or the DON as a whole with respect to the implementation of the program established under E.O. 12958 and its implementing directives.

**Senior Agency Official (SAO)** - The official designated by the agency head under section 5.6(c) of E.O. 12958 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

**Sensitive But Unclassified (SBU)** - Information that is originated within the DOS and warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the FOIA. (Previously "Limited Official Use" (LOU) in the DOS).

**Sensitive Information (Computer Security Act of 1987)** - Certain information in Federal Government AISs defined as "Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5 U.S.C. (Privacy Act), but which has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

**Sensitive Compartmented Information (SCI)** - Classified information concerning or derived from intelligence sources or methods, or analytical processes, that is required to be handled within formal access control systems established by the DCI.

**Short Title** - A brief, identifying combination of words, letters, or numbers applied to specific items of classified information.

**Signals Intelligence (SIGINT)** - Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

**Single Integrated Operational Plan (SIOP)** - A general war plan of the Joint Chiefs of Staff distributed by the Joint Staff Director of Strategic Target Planning.

**Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)** - Detailed Top Secret SIOP information that is extremely sensitive in nature.

**Source Document** - An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

**Special Access Program (SAP)** - Any DoD program or activity (as authorized in E.O. 12958) employing enhanced security measures (e.g., safeguarding or personnel adjudication requirements) exceeding those normally required for classified information at the same classification level which is established, approved, and managed as a DoD SAP.

**Systematic Declassification Review** - The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value per Chapter 33 of Title 44, U.S.C.

**Technical Data** - Recorded information related to experimental 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 or drawings, associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

**Technical documents** - Documents containing technical data or information.

**Technical Information** - Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

**Telecommunications** - The preparation, transmission, or communication of information by electronic means.

**Transmission** - Any movement of classified information from one place to another.

**Transportation** - A means of transport; conveyance of classified equipment or bulky shipments.

**Unauthorized Disclosure** - A communication or physical transfer of classified information to an unauthorized recipient.

**Unclassified Controlled Nuclear Information (UCNI)** - DoD or DOE unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material, equipment or facilities.

**U.S. and its Territorial Areas** - The 50 states, the District of Columbia, the Commonwealth of PR, and those possessions listed in the definition above.

**U.S. Citizens (including U.S. Nationals)** - A person born in one of the 50 States, its territories, possessions, Administrative and Commonwealth Areas, the DC, PR, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the U.S.). Naturalized U.S. citizen, or person born abroad of U.S. parent(s) and registered with an appropriate authority (U.S. Consul, DOS). For the purpose of the issuance of personnel security clearances, citizens of the Federated States of Micronesia and the Republic of the Marshall Islands are considered U.S. citizens.

**Upgrade** - To raise the classification of an item of information from one level to a higher one.

**Visitor Group** - Cleared DoD contractor employees assigned to a DON command, normally in support of a classified contract or program, who occupy or share Government spaces for a predetermined period.

**Waiver** - A written temporary relief, normally for a period of 1 year, from specific requirements imposed by this regulation, pending completion of actions which will result in conformance with the requirements. Interim compensatory security measures are required.

## ABBREVIATIONS

ACS - Access Control System

AIS - Automated Information System

AEA - Atomic Energy Act

AECS - Access Entry Control Systems

C - Confidential

CI - Counterintelligence

CIA - Central Intelligence Agency

CHINFO - Chief of Information

CMC - Commandant of the Marine Corps

CMS - Communications Security Material System

CNO - Chief of Naval Operations

CNR - Chief of Naval Research

CNWDI - Critical Nuclear Weapons Design Information

CO - Commanding Officer

COMNAVSECGRU - Commander, Naval Security Group

COMSEC - Communications Security

COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)

CSA - Cognizant Security Agency

CSP - Cryptographic Security Publication

CSS - Constant Surveillance Service

CUSR - Central U.S. Registry (NATO)

CVA - Central Verification Activity

DASD(S&IO) - Deputy Assistant Secretary of Defense, Security and Information Operations

DCI - Director, Central Intelligence

DCID - Director, Central Intelligence Directive

DCMS - Director, Communications Security Material System

DCS - Defense Courier Service

DEA - Drug Enforcement Agency

DIA - Defense Intelligence Agency

DLSC - Defense Logistics Services Center

DNI - Director of Naval Intelligence

DoD - Department of Defense

DODDAC - Department of Defense Damage Assessment Committee

DOE - Department of Energy

DON - Department of the Navy

DOS - Department of State

DSS - Defense Security Service (formerly Defense Investigative Service)

DTS - Defense Transportation System

DUSD(PS) - Deputy Under Secretary of Defense for Policy Support

E.O. - Executive Order

ESS - Electronic Security System

FAA - Federal Aviation Administration

FAD - Facility Access Determination

FBI - Federal Bureau of Investigation

FCL - Facility (Security) Clearance

FEDEX - Federal Express

FGI - Foreign Government Information

FI - Foreign Intelligence

FMS - Foreign Military Sales

FIPS - Federal Information Processing Standard

FOIA - Freedom of Information Act

FOUO - For Official Use Only

FRD - Formerly Restricted Data

GAO - General Accounting Office

GSA - General Services Administration

IC - Intelligence Community

IDE - Intrusion Detection Equipment

IDS - Intrusion Detection Systems

INFOSEC - Information Systems Security

IR&D - Independent Research and Development

ISP - Information Security Program

ISOO - Information Security Oversight Office

ISSM - Information Systems Security Manager

ISSO - Information Systems Security Officer

ITAR - International Traffic in Arms Regulation

JAG - Judge Advocate General of the Navy

JANAP - Joint Army, Navy, Air Force Publication

JCS - Joint Chiefs of Staff

LAA - Limited Access Authorization

MTMC - Military Traffic Management Command

NARA - National Archives and Records Administration

NATO - North Atlantic Treaty Organization

NAVY IPO - Navy International Programs Office

NCIS - Naval Criminal Investigative Service (Formerly NSIC, NISCOM and NIS)

NCISFO - Naval Criminal Investigative Service Field Office

NCISRA - Naval Criminal Investigative Service Resident Agency

NISP - National Industrial Security Program

NISPOM - National Industrial Security Program Operating Manual

NNPI - Naval Nuclear Propulsion Information

NSA - National Security Agency

NSG - Naval Security Group

NSN - National Stock Number

NWP - Naval Warfare Publication

OASD($C^3I$) - Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

OASD(PA) - Office of the Assistant Secretary of Defense (Public Affairs)

OCA - Original Classification Authority

OCC - Operations Center Columbus (formerly Defense Investigative Service Clearance Office (DISCO))

ONI - Office of Naval Intelligence

OPLOC - Operating Location (formerly Cognizant Security Office)

OSD - Office of the Secretary of Defense

PA - Privacy Act

PAO - Public Affairs Officer

PCL - Personnel Clearance Level

PCU - Premise Control Unit

PI - Preliminary Inquiry

PIN - Personal Identification Number

PM - Program Manager

POE - Port of Embarkation

PPP - Program Protection Plan

PRIN DIR (S&IO) - Principal Director, Security and Information Operations

PSS - Protective Security Service

RANKIN - Retrieval and Analysis of Navy Classified Information

RD - Restricted Data

ROI - Report of Investigation

S - Secret

SAC - Special Agent in Charge

SAO - Senior Agency Official

SAP - Special Access Programs

SBU - Sensitive But Unclassified

SCG - Security Classification Guide

SCI - Sensitive Compartmented Information

SCIF - Sensitive Compartmented Information Facility

SECDEF - Secretary of Defense

SECNAV - Secretary of the Navy

SF - Standard Form

SIOP - Single Integrated Operationals Plan

SIOP-ESI - Single Integrated Operational Plan-Extremely Sensitive Information

SJA - Staff Judge Advocate

SOIC - Senior Official of the Intelligence Community

SSO - Special Security Officer

SSSO - Subordinate Special Security Officer

TS - Top Secret

TSCA - Top Secret Control Assistant

TSCO - Top Secret Control Officer

UCNI - Unclassified Controlled Nuclear Information

UIC - Unit Identification Code

USMTF - U.S. Message Text Format

U.S.C. - United States Code

USPS - United States Postal Service

USSAN - United States Security Authority, NATO

# APPENDIX B

## FORMS

The forms listed below are used in conjunction with the ISP. These forms are procured through the Navy Supply System.

| Form Number/Name | Stock Number |
|---|---|
| DD 254 (12-90)<br>Contract Security Classification Specification | 0102-LF-011-5800 |
| DD 2501 (3-88)<br>Courier Authorization Card | 0102-LF-000-6900 |
| OPNAV 5511/10 (12-89)<br>Record of Receipt | 0107-LF-008-8000 |
| OPNAV 5511/51 (5-80)<br>Security Discrepancy Notice | 0107-LF-055-5355 |

**These forms are available only through GSA.**

| | |
|---|---|
| SF 700 (8-85)<br>Security Container Information | 7540-01-214-5372 |
| SF 701 (8-85)<br>Activity Security Checklist | 7540-01-213-7899 |
| SF 702 (8-85)<br>Security container Check Sheet | 7540-01-213-7900 |
| SF 703 (8-85)<br>Top Secret Cover Sheet | 7540-01-213-7901 |
| SF 704 (8-85)<br>Secret Cover Sheet | 7540-01-213-7902 |
| SF 705 (8-85)<br>Confidential Cover Sheet | 7540-01-213-7903 |
| SF 706 (1-87)<br>Top Secret Label | 7540-01-207-5536 |

| | |
|---|---|
| SF 707 (1-87)<br>Secret Label | 7540-01-207-5537 |
| SF 708 (1-87)<br>Confidential Label | 7540-01-207-5538 |
| SF 709 (1-87)<br>Classified Label | 7540-01-207-5540 |
| SF 710 (1-87)<br>Unclassified Label | 7540-01-207-5539 |
| SF 711 (1-87)<br>Data Descriptor Label | 7540-01-207-5541 |
| SF 712 (10-87)<br>Classified SCI | 7540-01-267-1158 |
| OF 89 (9-98)<br>Maintenance Record for<br>Security Containers/Vaults | Local reproduction<br>authorized |

Note: The OF 89 may be found on the GSA website at www.gsa.gov/forms

# APPENDIX C

## REPORT CONTROL SYMBOLS

| Title | Report Symbol | Paragraph |
|---|---|---|
| Preliminary Inquiry into Compromise or Subjection to Compromise of Classified Information | OPNAV 5510-6B | 12-3 |
| Report of JAG Manual Investigation into Compromise of Classified Information | OPNAV 5510-6C | 12-9 |
| Report of Compromise through Public Media | OPNAV 5510-6E | 12-18 |
| Security Discrepancy Notice | OPNAV 5510-6G | 12-19 |
| Report Emergency Destruction of Classified Material | OPNAV 5510-6N (MIN: Considered) | Ex.2B-2 |
| Agency Information Security Program Data | 0230-NAR-AN | 1-3 |

# INDEX

PARAGRAPH

## A

ABBREVIATIONS AND DEFINITIONS . . . . . App A
ACCESS
  Congressional staff . . . . . 9-14
  Facility Access Determination (FAD) Program . . . . . 11-6
  Meetings . . . . . 7-12
  Visits . . . . . 7-11
ACCESS CONTROLS AND IDS . . . . . 10D-1
ACCOUNTABILITY
  Accountability of classifiers . . . . . 4-10
ACCOUNTING AND CONTROL
  Confidential . . . . . 7-5
  NATO classified material . . . . . 7-7
  NWPs . . . . . 7-7
  Requirements for classified material . . . . . 7-1
  Secret . . . . . 7-4
  Special types of classified and controlled unclassified
    information . . . . . 7-7
  Top Secret . . . . . 7-3
  Working papers . . . . . 7-6
ADDRESSING CLASSIFIED MATERIAL FOR SHIPMENT . . . . . 9-9
ALTERNATIVE OR COMPENSATORY CONTROL MEASURES . . . . . 7-8
ARCHIVIST OF THE UNITED STATES . . . . . 4-24
ASSIGNING DISTRIBUTION STATEMENTS ON TECHNICAL
  DOCUMENTS . . . . . Exh 8A
ASSIST VISITS . . . . . 2-11
ASSOCIATED MARKINGS . . . . . 6-7
ATOMIC ENERGY ACT OF 1954 . . . . . 1-1
AUTHORITY TO DOWNGRADE, DECLASSIFY OR MODIFY
  CLASSIFIED INFORMATION . . . . . 4-19
AUTHORIZATION TO ESCORT OR HANDCARRY CLASSIFIED
  INFORMATION . . . . . 9-12
AUTHORIZATION TO HANDCARRY CLASSIFIED INFORMATION
  IN A TRAVEL STATUS . . . . . 9-13
AUTHORIZED INTELLIGENCE CONTROL MARKINGS . . . . . 6-12
AUTOMATED INFORMATION SYSTEMS (AISs)
  Accountability and control . . . . . 7-7
  Destruction . . . . . 10-17
  Dissemination . . . . . 8-4
  ISSM . . . . . 2-7
  ISSO . . . . . 2-7
  Loss or compromise . . . . . 12-8
  Marking . . . . . 6-33, 6-34
AUTOMATIC DECLASSIFICATION . . . . . 4-21

B

BASIC MARKING REQUIREMENTS . . . . . 6-1
BID AND PROPOSAL (B&P) . . . . . 4-16
BLUEPRINTS . . . . . 6-27
BRIEFINGS (see INFORMATION SECURITY)
BULK SHIPMENTS . . . . . 9-7
BURN BAGS . . . . . 10-19

C

CARE OF SPACES DURING WORKING HOURS . . . . . 7-9
CENTRAL U.S. REGISTRY (CUSR) . . . . . 1-4, 2-5
CHAIN OF COMMAND . . . . . 1-2
CHANGES TO EXISTING CLASSIFIED DOCUMENTS . . . . . 6-19
CHARTS . . . . . 6-27
CHIEF OF NAVAL OPERATIONS (ISP responsibilities)
(N09N) . . . . . 1-4, 1-5, 4-4, 4-22, 5-3
(N09N2) . . . . . 1-5, 5-3, 7-12, 12-8, 12-18
(N09N3) . . . . . 10-1, 10-16
(N2) . . . . . 1-5
(N2E) . . . . . 1-5
(N514) . . . . . 1-1
(N6) . . . . . 1-5
(N643) . . . . . 1-5
(N8) . . . . . 1-5
(N89) . . . . . 1-1, 1-5
CLASSIFICATION
By compilation . . . . . 6-18
Challenges . . . . . 4-12
Conflicts, resolution of . . . . . 4-13
Derivative . . . . . 4-9
Duration of . . . . . 4-8
Equivalents . . . . . 4-17, Exh 6C
FGI . . . . . 4-17
Guides . . . . . 5-2, 5-3
Limitations on . . . . . 4-11
Original . . . . . 4-3
Previously unclassified information . . . . . 4-11, 4-26
Prohibitions . . . . . 4-11
Tentative . . . . . 4-14
Upgrading . . . . . 4-26
CLASSIFICATION AUTHORITY
Accountability . . . . . 4-10
Derivative . . . . . 4-9
Original . . . . . 4-4
CLASSIFICATION CHALLENGES . . . . . 4-12
CLASSIFICATION BY COMPILATION . . . . . 6-18
CLASSIFICATION GUIDES (See SECURITY CLASSIFICATION GUIDES)

C

CLASSIFICATION LEVELS . . . . . 4-2
CLASSIFICATION MANAGEMENT . . . . . 4-1
CLASSIFIED AREAS, VISITS AND MEETINGS . . . . . 7-11, 7-12
CLASSIFIED BULKY FREIGHT SHIPMENTS . . . . . 9-7
CLASSIFIED DOCUMENT MARKING SAMPLES . . . . . Exh 6A
CLASSIFIED INFORMATION
  Cover Sheets . . . . . 9-11
  Criteria for classifying . . . . . 4-7
  Custodial responsibility . . . . . 12-9
  Disposition of by deactivated commands . . . . . 10-21
  Disposition of by persons leaving the Navy . . . . . 7-1
  Documentation required to handcarry or escort
    aboard commercial aircraft . . . . . 9-13
  Handcarry or escort aboard commercial aircraft . . 9-12, 9-13
  Handcarry within a command . . . . . 9-11
  Improper transmission of . . . . . 12-19
  Located in foreign countries . . . . . 12-6
  Marking of (see MARKING)
  Removal from secure area . . . . . 10-10
  Turned over to friendly foreign governments . . . . . 10-21
  Transmission/transportation . . . . . 9-1
  Unauthorized disclosure . . . . . 12-1, 12-2
CLASSIFIED INFORMATION TRANSFERRED TO THE DON . . . . . 4-25
CLASSIFIED MATERIAL . . . . . 1-1, 6-1
CLASSIFIED MEETINGS . . . . . 7-12
CLASSIFIED MESSAGE MARKING SAMPLES . . . . . Exh 6B
CLASSIFIED STORAGE REQUIREMENTS . . . 10-1, 10-3, 10-10, 10-16
CLASSIFIED VISITS . . . . . 7-11
CLASSIFIED WASTE . . . . . 7-9, 10-19
CLASSIFIER (see CLASSIFICATION AUTHORITY)
CLASSIFYING FROM SOURCE DOCUMENTS WITH OLD
  DECLASSIFICATION INSTRUCTIONS . . . . . 6-23
"CLEAN-OUT" DAY . . . . . 10-17
CLEARED DoD CONTRACTOR OPERATIONS . . . . . 11-1, 11-2
CLEARANCE UNDER THE NISP . . . . . 11-4
CLEARANCE VERIFICATION ACTIVITY (CVA) . . . . . 11-13
CODE WORDS
  Assignment . . . . . 6-17
  Marking . . . . . 6-17
COMBAT OPERATIONS . . . . . 1-2
COMBINATIONS
  Changes . . . . . 10-12
  Change envelope . . . . . 10-12
  Keys and padlocks . . . . . 10-13
  Storage of . . . . . 10-12

C

COMMAND
  COR . . . . . 2-6
  Emergency destruction supplement . . . . . Exh 2B
  Emergency plan . . . . . Exh 2B
  ISSM . . . . . 2-7
  ISSO . . . . . 2-7
  Security assistants . . . . . 2-4
  Security instruction . . . . . Exh 2A
  Security Manager . . . . . 2-2
  Security Officer . . . . . 2-9
  SSO . . . . . 2-8
  SSSO . . . . . 2-8
  TSCA . . . . . 2-3, 2-4
  TSCO . . . . . 2-3
COMMANDANT MARINE CORPS (CMC) . . . . . 1-5
  CMC (Code ARS) . . . . . 1-5
  CMC (Code CIZ) . . . . . 1-5
COMMANDER, NAVAL SECURITY GROUP (COMNAVSECGRU) . . . . 1-4, 1-5
COMMANDING OFFICER . . . . . 2-1, 12-2
COMMUNICATIONS SECURITY (COMSEC)
  Destruction of . . . . . 10-17
  Dissemination . . . . . 8-4
  Loss or compromise . . . . . 12-8
  Marking . . . . . 6-11
  Safeguarding . . . . . 7-7
  Telephone . . . . . 9-6
  Traffic review . . . . . 12-8
  Transmission/transportation . . . . . 9-5
COMPROMISE . . . . . 12-1
  Custodial responsibility . . . . . 12-3, 12-9
  Damage assessment of . . . . . 12-17
  Deliberate . . . . . 12-8
  Public media . . . . . 12-18
  Reporting responsibilities . . . . . 12-2
  Special types of information and equipment . . . . . 12-8
CONFERENCES (see CLASSIFIED MEETINGS)
CONFLICT BETWEEN A SOURCE DOCUMENT AND AN SCG . . . . . 5-6
CONGRESS
  Dissemination to . . . . . 8-6
CONSTANT SURVEILLANCE SERVICE (CSS) . . . . . 9-4
CONTAINERS (See SECURITY CONTAINERS)
CONTRACT OFFICERS REPRESENTATIVE (COR) . . . . . 2-6, 11-8
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
  (DD 254) . . . . . 11-7, Exh 11A
CONTRACTOR
  Badges . . . . . 11-9
  Disclosure of classified information to . . . . . 11-13

C

CONTRACTOR (Con't)
Prohibited release of intelligence to . . . . . 11-15
Release of intelligence information to . . . . . 11-14
Sanitization of intelligence information for . . . . . 11-16
CONTRACTOR FACILITY CLEARANCES . . . . . 11-11
CONTROL
Dissemination . . . . . 6-11
Markings . . . . . 6-11, 6-12
Reproduction . . . . . 6-11, 7-13
CONTROL MEASURES . . . . . 7-1, 7-2
Alternative or compensatory . . . . . 7-8
CONTROLLED UNCLASSIFIED INFORMATION . . . . . 1-1
Dissemination . . . . . 8-4
Destruction . . . . . 10-20
Loss or compromise . . . . . 12-8
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
CORRESPONDENCE AND LETTERS OF TRANSMITTALS . . . . . 6-24
COURIERS
Classified . . . . . 9-11
COVER SHEETS . . . . . 7-9, 9-11
CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)
Destruction . . . . . 10-17
Dissemination . . . . . 8-4
Loss or compromise . . . . . 12-8
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
CRYPTOLOGY . . . . . 4-22, 6-11

D

DAMAGE ASSESSMENT . . . . . 12-17
DECLASSIFICATION
Authority . . . . . 4-19
Automatic . . . . . 4-21
By ISOO . . . . . 4-20
FGI . . . . . 4-22
Instructions . . . . . 6-10, 6-19
Mandatory Review . . . . . 4-23
Marking . . . . . 6-10, 6-19
National Archives review . . . . . 4-24, 4-25
Notification of . . . . . 4-26
Systematic Review . . . . . 4-22
DEFENSE COURIER SERVICE (DCS) . . . . . 9-2
DEFENSE INTELLIGENCE AGENCY (DIA) . . . . . 1-4

D

DEFENSE SECURITY SERVICE (DSS) . . . . . 11-3
DSS and command security oversight of cleared DoD contractor operations . . . . . 11-5
DEFINITIONS AND ABBREVIATIONS . . . . . App A
DEPARTMENT OF DEFENSE (DoD)
Deputy Under Secretary of Defense for Policy Support (DUSD(PS)) . . . . . 1-4
Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence (OASD(C3I)) . . . . . 1-4
Under Secretary of Defense for Policy (DUSD(P)) . . . . . 1-4
DEPARTMENT OF STATE (DOS) COURIER SYSTEM . . . . . 9-9
DEPARTMENT OF THE NAVY (DON)
DON Chief Information Officer, Office of the Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN(RD&A)) . . . . . 1-5
DON Senior Agency Official . . . . . 1-5
Liaison with ASD . . . . . Exh 8A
Program management . . . . . 1-5
DERIVATIVE CLASSIFICATION (See CLASSIFICATION AUTHORITY)
DERIVATIVE CLASSIFIER (See CLASSIFICATION AUTHORITY)
DESTRUCTION
Burn bags . . . . . 10-19
Central destruction facility . . . . . 10-19
Classified . . . . . 10-17
Controlled unclassified information . . . . . 10-20
Emergency plan and supplement . . . . . Exh 2B
Equipment . . . . . 10-18
Methods . . . . . 10-18
Procedures . . . . . 10-19
Records . . . . . 10-19
Reporting emergency destruction . . . . . Exh 2B
Standards . . . . . 10-18
Unclassified-limited distribution documents . . . . . Exh 8A
DIRECTOR CENTRAL INTELLIGENCE (DCI) . . . . . 1-3
DIRECTOR NAVAL INTELLIGENCE (DNI) . . . . . 1-5
DIRECTOR NAVAL CRIMINAL INVESTIGATIVE SERVICE (DIRNCIS) . . . . . 1-5
DIRECTOR, NAVY INTERNATIONAL PROGRAMS OFFICE (NAVY IPO) . . . . . 1-5
DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO) . . . . . 1-3
DIRECTOR, SECURITY DIRECTORATE/SSO NAVY (ONI-5) . . . 1-5, 2-8
DIRECTOR SPACE, INFORMATION WARFARE, COMMAND AND CONTROL (CNO N6) . . . . . 1-5

D

DISCLOSURE OF INFORMATION TO FOREIGN GOVERNMENTS
AND INTERNATIONAL ORGANIZATIONS . . . . . 7-12, 8-1
DISCREPANCY NOTICE . . . . . Exh 12E
DISPOSITION OF CLASSIFIED INFORMATION FROM COMMANDS
REMOVED FROM ACTIVE STATUS OR TURNED OVER TO FRIENDLY
FOREIGN GOVERNMENTS . . . . . 10-21
DISSEMINATION
Basic policy . . . . . 8-1
Categories of information requiring ASD(PA)
approval prior to public release . . . . . Exh 8B
Congress . . . . . 8-6
Controlled unclassified information . . . . . 8-4
Foreign governments and international
organizations . . . . . 8-1
Independent Research and Development (IR&D) . . . . . Exh 8A
Intelligence . . . . . 8-5, 11-15
International Traffic in Arms (ITAR) . . . . . Exh 8B
Non-DoD information . . . . . 8-1
Prepublication review . . . . . 8-8
Procedures for assigning distribution statements . . . Exh 8A
Proprietary information . . . . . Exh 8A
Secret and confidential . . . . . 8-3
Special types of classified information . . . . . 8-4
Technical documents . . . . . 8-7
"Third agency rule" . . . . . 8-5
Top Secret . . . . . 8-2
DISTRIBUTION STATEMENTS ASSIGNED TO TECHNICAL
DOCUMENTS . . . . . Exh 8A
DoD SECURITY PROGRAM MANAGEMENT . . . . . 1-4
DOCUMENT . . . . . 6-1
DON SECURITY PROGRAM MANAGEMENT . . . . . 1-5
DOWNGRADING
Authority . . . . . 4-19
FGI . . . . . 4-22
Marking . . . . . 6-10
Notification . . . . . 4-26
Remarking requirements . . . . . 6-22
DURATION . . . . . 6-22
Classification . . . . . 4-8
DUTIES (security related)
Collateral . . . . . 2-5
Commanding Officer . . . . . 2-1
Command COR . . . . . 2-6
ISSM . . . . . 2-7
ISSO . . . . . 2-7
Security assistants . . . . . 2-4
Security Officer . . . . . 2-9

D

DUTIES (security related) (Con't)
Security Manager . . . . . 2-2
SSO . . . . . 2-8
TSCO . . . . . 2-3

E

EDUCATION (see INFORMATION SECURITY EDUCATION)
ELECTRICALLY ACTUATED LOCKS . . . . . 10-7
ELECTRICALLY TRANSMITTED MESSAGES . . . . . 6-25, Exh 6B
ELECTRONIC SECURITY SYSTEM (ESS) . . . . . 10-16
EMERGENCY DESTRUCTION PLAN AND SUPPLEMENT . . . . . Exh 2B
END-OF-DAY SECURITY CHECKS . . . . . 7-10
ENVELOPES
Addressing . . . . . 9-9
Classified combination . . . . . 10-12
Mailing . . . . . 9-8, 9-9
EQUIVALENT FOREIGN SECURITY CLASSIFICATIONS . . . . . Exh 6C
ESCORTING OR HANDCARRYING CLASSIFIED INFORMATION . . . . . 9-11
ESCORTING CLASSIFIED INFORMATION ABOARD COMMERCIAL
AIRCRAFT . . . . . 9-11, 9-13
ESCORT OR HANDCARRY OF CLASSIFIED INFORMATION TO THE
SENATE . . . . . 9-14
EXCEPTIONS . . . . . 1-2, 6-1
EXERCISE TERMS . . . . . 6-17
FACILITY ACCESS DETERMINATION (FAD) PROGRAM . . . . . 11-6
FACSIMILE (see TRANSMISSION/TRANSPORTATION)
FEDERAL BUREAU OF INVESTIGATION (FBI) . . . . . 1-3
FILES, FOLDERS, AND GROUPS OF DOCUMENTS . . . . . 6-26
FILING CABINETS . . . . . 10-6
FOR OFFICIAL USE ONLY (FOUO) . . . . . 1-1, 4-2
Destruction . . . . . 10-20
Dissemination . . . . . 8-4
Marking . . . . . 6-5, 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
FOREIGN GOVERNMENTS
Correspondence to . . . . . Exh 9A
Dissemination of intelligence . . . . . 8-5
Military sales to . . . . . Exh 9A
Transmission/transportation of classified
Information to . . . . . Exh 9A
FOREIGN GOVERNMENT INFORMATION (FGI)
Classification and duration . . . . . 4-17
Declassification/downgrading . . . . . 4-22
Destruction . . . . . 7-7
Dissemination . . . . . Exh 8A

F

FOREIGN GOVERNMENT INFORMATION (FGI) (Con't)
Equivalents . . . . . Exh 6C
Loss or compromise . . . . . 12-8
Marking . . . . . 6-15
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . Exh 9A
FOREIGN INTELLIGENCE AGENCY . . . . . 12-8
FOREIGN RELATIONS SERIES . . . . . 4-27
FORMATS
Classified marking . . . . . Exh 6A
JAGMAN appointment letter . . . . . Exh 12C
JAGMAN investigation reporting . . . . . Exh 12D
PI reporting . . . . . Exh 12A
PI message reporting . . . . . Exh 12B
SCGs . . . . . 5-2
USMTF classified message . . . . . Exh 6B
FOREIGN MILITARY SALES (FMS) . . . . . Exh 9A
FOREIGN "RESTRICTED" INFORMATION . . . . . 4-17
Destruction . . . . . 10-17
Dissemination . . . . . Exh 8A
Marking . . . . . 6-15
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . Exh 9A
FORMERLY RESTRICTED DATA (FRD)
Declassification . . . . . 1-5
Dissemination . . . . . 8-4
Loss or compromise . . . . . 12-8
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
FORMS . . . . . 2-12, App B
FREEDOM OF INFORMATION ACT (FOIA) REQUESTS . . . . . 4-23

G

GENERAL SERVICE ADMINISTRATION (GSA) . . . . . 10-2
GSA SECURITY CONTAINERS
Approved . . . . . 10-3
Combinations . . . . . 10-12
Maintenance . . . . . 10-15, Exh 10C
Non-approved . . . . . 10-3, 10-6, 10-9
Operating inspections . . . . . 10-15
Procurement . . . . . 10-4
Repair . . . . . 10-15
Residential . . . . . 10-10
Securing . . . . . 10-14

G

GSA SECURITY CONTAINERS (Con't)
Specialized . . . . . 10-8
Standards . . . . . 10-2
GUIDELINES FOR COMMAND SECURITY INSTRUCTION . . . . . Exh 2A
GUIDES (see SECURITY CLASSIFICATION GUIDES)

H

HANDCARRYING AND ESCORTING CLASSIFIED INFORMATION
Authorization . . . . . 9-12
Authorization aboard commercial aircraft . . . . . 9-13
Courier briefings . . . . . 9-11
Documentation required . . . . . 9-12, 9-13
DOS Diplomatic Courier Service . . . . . 9-9
General provisions . . . . . 9-11
Outside CONUS . . . . . Exh 9A
Receipting . . . . . 9-10
Restrictions . . . . . 9-12
Storage during intermediate stops . . . . . 9-11
To the Senate . . . . . 9-14
Within the command . . . . . 9-11

I

IDENTIFICATION
Classified courier . . . . . 9-13
Contractor . . . . . 11-9, 11-12
Courier card (DD 2501) . . . . . 9-12
IDS AND ACCESS CONTROLS . . . . . Exh 10D
INFORMATION EXEMPTED FROM MANDATORY DECLASSIFICATION
REVIEW . . . . . 4-24
IMPROPER TRANSMISSION . . . . . 12-19
INDUSTRIAL SECURITY (cleared contractors)
Authority, basic policy and classification
guidance . . . . . 11-1, 11-2
Clearance under the NISP . . . . . 11-4
Clearance Verification Activity (CVA) . . . . . 11-13
Contract couriers, escorts or handcarriers . . . . . 11-12
Contracting Officer's Representative (COR) . . . . . 2-6, 11-8
Contract Security Classification Specification
(DD 254) . . . . . 11-7, Exh 11A
Contractor badges . . . . . 11-9
Defense Security Service (DSS) . . . . . 11-3
Disclosure of classified to contractors . . . . . 11-13
Dissemination of classified or technical
information . . . . . Exh 8A
DSS, Operations Center Columbus (OCC) . . 11-3, 11-11, 11-13
DSS Operating Locations (OPLOCS) . . . . . 11-3, 11-12

I

INDUSTRIAL SECURITY (cleared contractors) (Con't)
DSS and Security Oversight of cleared DoD contractor Operations . . . . . 11-5
FAD Program . . . . . 11-6
FCL . . . . . 11-3, 11-4, 11-5, 11-11, 11-13
Joint Certification Program . . . . . 11-13
Letter . . . . . 11-12
Military Critical Technical Data Agreement (DD 2345) . . . . . 11-13
NISP . . . . . 1-2
Off-site locations . . . . . 11-5
Overseas locations . . . . . 11-5
Program Protection Plan (PPP) . . . . . 11-1
Prohibited release of intelligence . . . . . 11-15
Release of Intelligence to contractors . . . . . 11-14
Sanitization of intelligence information . . . . . 11-16
Shipboard . . . . . 11-5
Shore installations . . . . . 11-5
Transmission/transportation . . . . . 11-12
INDEPENDENT RESEARCH AND DEVELOPMENT INFORMATION (IR&D)/ BID AND PROPOSAL (B&P) . . . . . 4-16, 6-14
INDUSTRIAL SECURITY LETTER (ISL) . . . . . 11-12
INFORMATION SECURITY EDUCATION . . . . . 3-3
INFORMATION SECURITY PROGRAM (ISP)
Alternative or compensatory control measures . . . . . 1-2
Applicability and scope . . . . . 1-1
Command-imposed requirements . . . . . 2-1
Compliance . . . . . 1-1
DoD security program management . . . . . 1-4
DON security program management . . . . . 1-5
Exceptions and waivers to the . . . . . 1-2
Implementation of . . . . . 2-1
Management responsibility and authority for . . . . . 2-1
National authorities . . . . . 1-3
Policy guidance . . . . . 1-2
INFORMATION SECURITY OVERSIGHT OFFICE (ISOO) . . . . . 1-3
INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM . . . . . 1-5
INFORMATION SYSTEM SECURITY MANAGER (ISSM) . . . . . 2-7
INFORMATION WARFARE (See (CNO (N6) and CNO (N643))
INSPECTIONS (Security) . . . . . 2-11
Checklist . . . . . Exh 2C
Requirements for . . . . . 2-11
INSTRUCTION (See COMMAND)
INTELLIGENCE CONTROL MARKINGS . . . . . 6-12
INTERAGENCY INTELLIGENCE MEMORANDA . . . . . 11-14
INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL (ISCAP) . . . . . 4-12, 4-23
INTERIOR PAGE MARKINGS . . . . . 6-4

I

INTERNATIONAL TRAFFIC IN ARMS (ITAR) . . . . . Exh 8B
INTRUSION DETECTION SYSTEMS (IDS) . . . . . Exh 10D
INVENTORIES
  Special types of classified and controlled unclassified information . . . . . 7-7
  Top Secret . . . . . 7-3
INVESTIGATIVE ASSISTANCE . . . . . 12-11

J

JAGMAN INVESTIGATIONS
  Appointment letter . . . . . 12-10, Exh 12C
  Assistance . . . . . 12-10, 12-11
  Classification . . . . . 12-12
  Damage assessments . . . . . 12-17
  Endorsements . . . . . 12-14
  Format . . . . . Exh 12D
  Initiation . . . . . 12-10
  Notifications . . . . . 12-2, 12-8
  OCA Reviews . . . . . 12-15, 12-16
  Requirements . . . . . 12-7, 12-14
  Results . . . . . 12-13
  Review by superiors . . . . . 12-14
  Security reviews . . . . . 12-15

K

KEY CONTROL . . . . . 10-13
KEY-OPERATED HIGH SECURITY PADLOCKS (See LOCKS)

L

LETTERS OF TRANSMITTAL . . . . . 6-24
LIMITATIONS ON CLASSIFYING . . . . . 4-11
LOCKS
  Combination . . . . . 10-12
  Cipher . . . . . 10-7
  Key-operated high security padlocks . . . . . 10-13
  Electrically actuated . . . . . 10-7
  Maintenance of . . . . . 10-15
  Operating inspections . . . . . 10-15
  Repair of . . . . . 10-15
  Replacement of combination . . . . . 10-11
MANDATORY DECLASSIFICATION REVIEW . . . . . 4-23
  Information exempted from . . . . . 4-24
MAPS . . . . . 6-27

M

MARINE CORPS
Program management responsibilities . . . . . 1-5
MARKING
AIS equipment . . . . . 6-33
AIS media . . . . . 6-33
AIS printouts . . . . . 6-34
Basic policy . . . . . 6-1
Blueprints . . . . . 6-27, Exh 6A
Containers . . . . . 6-28, 6-30, 6-31, Exh 6A
Captions . . . . . 6-5, Exh 6A
Changes to existing classified documents . . . . . 6-19
Charts . . . . . 6-27, Exh 6A
"Classified by line" . . . . . 6-8, Exh 6A
Classified pages removed from AIS printouts . . 6-35, Exh 6A
CNWDI . . . . . 6-11, Exh 6A
Code words . . . . . 6-17
Controlled unclassified information . . . . . 6-11
Compilation documents . . . . . 6-18
Component parts of a classified document . . . . . 6-21
COMSEC . . . . . 6-11
Correspondence . . . . . 6-24
Date of origin . . . . . 6-2, Exh 6A
Department of State (DOS) sensitive but unclassified
information . . . . . 6-11
"Derived from" line . . . . . 6-9, Exh 6A
Derivatively classified documents . . . . . 6-9, Exh 6A
Dissemination and reproduction notices . . . . . 6-11, Exh 8A
DoD UCNI . . . . . 6-11
Documents containing both original and derivative
classification . . . . . 6-8, Exh 6A
Documents classified from source documents with old
declassification instructions . . . . . 6-23
Documents produced by AIS equipment . . . . . 6-34, Exh 6A
DON command (originating) . . . . . 6-2, Exh 6A
Downgraded or declassified documents . . . . . 6-22, Exh 6A
Drawings . . . . . 6-27
DEA sensitive information . . . . . 6-11
Electrically transmitted messages . . . . . 6-25, Exh 6B
Exceptions . . . . . 6-1
Exercise terms . . . . . 6-17
Files and folders . . . . . 6-26
Folded classified documents . . . . . 6-27, Exh 6A
For Official Use Only (FOUO) . . . . . 6-11, Exh 6A
Formerly Restricted Data (FRD) . . . . . 6-11, Exh 6A
Foreign Government "RESTRICTED" information . . . 6-11, 6-15
Foreign Government Information (FGI) . . . . . 6-15, Exh 6A

M

MARKING (Con't)
Foreign security classification designation equivalents . . . . . 6-15, Exh 6C
Groups of documents . . . . . 6-26, 6-29
Independent Research and Development (IR&D) . . . . . 6-14
Intelligence control markings . . . . . 6-12, Exh 6A
Interior pages . . . . . 6-4, Exh 6A
Letters of transmittal . . . . . 6-24, Exh 6A
Maps . . . . . 6-27, Exh 6A
Microforms . . . . . 6-32
Miscellaneous classified . . . . . 6-35
Motion picture films . . . . . 6-30, Exh 6A
"Multiple Source" documents . . . . . 6-8, 6-9, Exh 6A
NATO documents . . . . . 6-11, 6-15
Negatives . . . . . 6-28
Nicknames . . . . . 6-17
Naval Nuclear Propulsion Information (NNPI) . . 6-11, Exh 6A
Originally classified information . . . . . 6-8, Exh 6A
Originating Agency Determination Required (OADR) . 6-15, 6-23
Overall and page classification level . . . . . 6-3, Exh 6A
Paragraphs . . . . . 6-5, Exh 6A
Patent Secrecy Act information . . . . . 6-13
Photographs . . . . . 6-28, Exh 6A
Placement of associated markings . . . . . 6-7, Exh 6A
Portions . . . . . 6-5, Exh 6A
"Reason" line . . . . . 6-8, Exh 6A
Remarking upgraded, downgraded or declassified documents . . . . . 6-22
Removable AIS storage media . . . . . 6-33, Exh 6A
Restricted Data (RD) . . . . . 6-11, Exh 6A
Rolled classified documents . . . . . 6-27, Exh 6A
SIOP/SIOP-ESI . . . . . 6-11
Slides . . . . . 6-29, Exh 6A
Sound recordings . . . . . 6-31, Exh 6A
"Source Marked "OADR" . . . . . 6-23
Subjects . . . . . 6-6, Exh 6A
Subparagraphs . . . . . 6-5, Exh 6A
Training and test documents . . . . . 6-20, Exh 6A
Translations . . . . . 6-16, Exh 6C
Transparencies . . . . . 6-29, Exh 6A
Titles . . . . . 6-6, Exh 6A
Upgraded, downgraded, or declassified information . . . . . 6-22
Videotapes . . . . . 6-30, Exh 6A
Waivers . . . . . 1-2, 6-5
MEDIA COMPROMISES (see PUBLIC MEDIA COMPROMISES)
MEETINGS (see CLASSIFIED MEETINGS)

M

MICROFORMS . . . . . 6-32
MILITARY EQUIPMENT (See FOREIGN MILITARY SALES)
MISCELLANEOUS CLASSIFIED MATERIAL . . . . . 6-35
MOTION PICTURE FILMS . . . . . 6-30
MULTIPLE SOURCE DOCUMENTS . . . . . 6-8, 6-9
MULTI-SERVICE INTEREST . . . . . 5-5

N

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) . . . 4-25
NATIONAL AUTHORITIES FOR SECURITY MATTERS . . . . . 1-3
NATIONAL DISCLOSURE POLICY (NDP) . . . . . 1-4
NATIONAL FOREIGN INTELLIGENCE BOARD (NFIB) . . . . . 1-3, 1-4
NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) . . . . . 1-1
NATIONAL INTELLIGENCE ESTIMATES (NIES) . . . . . 11-14
NATIONAL SECURITY AGENCY (NSA) . . . . . 1-4, 10-17, 12-8
Approved destruction equipment . . . . . 10-17
COMSEC issues . . . . . 12-8
NATIONAL SECURITY COUNCIL (NSC) . . . . . 1-3
NATIONAL SECURITY INFORMATION (NSI) . . . . . 1-3, 4-1
NATO (See NORTH ATLANTIC TREATY ORGANIZATION (NATO))
NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS). . 1-5, 12-9, 12-11
NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) . . . . . 1-1, 4-18
Destruction . . . . . 10-20
Dissemination . . . . . 8-4
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
NAVAL NUCLEAR PROPULSION PROGRAM . . . . . 4-18
NAVAL NUCLEAR REACTOR PROGRAM . . . . . 4-18
NAVAL SECURITY GROUP COMMAND (NAVSECGRU) . . . . . 1-4, 1-5
NAVAL WARFARE PUBLICATIONS (NWPs) . . . . . 2-5
Custodian . . . . . 2-5
Safeguarding . . . . . 7-7
NAVY DEFENSIVE INFORMATION WARFARE/INFORMATION
SYSTEMS SECURITY BRANCH (CNO N643) . . . . . 1-5
NAVY INTERNATIONAL PROGRAMS OFFICE (NAVY IPO) . . . . 1-5, 7-12
NAVY SCIENTIFIC AND TECHNICAL PROGRAM . . . . . Exh 8A
NEGATIVES . . . . . 6-28
NEWS MEDIA (See PUBLIC MEDIA COMPROMISE)
NEWSLETTER (Information and Personnel Security) . . . . . 1-5
NICKNAMES . . . . . 6-17
NON GSA-APPROVED SECURITY CONTAINERS . . . . . 10-9
NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN) (See INTELLIGENCE
CONTROL MARKINGS)

N

NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION . . . 1-1
Central U.S. Registry . . . . . 1-4, 2-5
Classified and unclassified . . . . . 1-1
Control officer . . . . . 2-5
Dissemination . . . . . 8-4
Marking of . . . . . 6-11
Restricted . . . . . 1-1
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
United States Security Authority NATO (USSAN) . . . . . 1-4
NOTIFICATION OF CLASSIFICATION CHANGES . . . . . 4-26

O

OCA TRAINING . . . . . 4-6
OFFICE OF NAVAL INTELLIGENCE (ONI) . . . . . 1-5
(ONI-5) . . . . . 1-5
OPERATING INSPECTIONS . . . . . 10-15
OPERATING LOCATION (OPLOC) . . . . . 11-3, 11-12
ORIGINAL CLASSIFICATION . . . . . 4-3
Criteria, Principles, and Considerations . . . . . 4-7
Duration . . . . . 4-8
ORIGINAL CLASSIFICATION AUTHORITIES (OCAs) . . . . . 4-4
OCA Training and indoctrination . . . . . 4-6
Resolutions of conflicts between OCAs . . . . . 4-13
Listing . . . . . Exh 4A
ORIGINAL CLASSIFICATION AUTHORITY . . . . . 4-4
Requests for . . . . . 4-5
ORIGINAL CLASSIFICATION REVIEWS . . . . . 12-13, 12-15
ORIGINATING AGENCY'S DETERMINATION REQUIRED (OADR) . . . . 6-15
OVERALL CLASSIFICATION LEVEL MARKING . . . . . 6-3

P

PADLOCKS . . . . . 10-3, 10-12, 10-13
PADLOCK CONTROL . . . . . 10-13
PATENT SECRECY ACT OF 1952 . . . . . 4-15, 6-13
PATENT SECRECY INFORMATION . . . . . 4-15
PERIODIC REVIEW OF SCGs . . . . . 5-4
PERSONNEL SECURITY PROGRAM . . . . . 1-5
PHOTOGRAPHS . . . . . 6-28
PORTION MARKINGS . . . . . 6-5
PRELIMINARY INQUIRY (PI) . . . . . 12-3
Appointment letter . . . . . 12-4
Classification of PI message or letter . . . . . 12-6
Conclusions of . . . . . 12-7
Contents . . . . . 12-5

P

PRELIMINARY INQUIRY (PI) (Con't)
Formats (message or letter) . . . . . Exhs 12A, 12B
Initiation . . . . . 12-4
Notifications . . . . . 12-2, 12-4, 12-7
Process . . . . . 12-3
Reporting requirements . . . . . 12-7, 12-8
PREPARING CLASSIFIED INFORMATION FOR SHIPMENT . . . . . 9-8
PREPUBLICATION REVIEW . . . . . 8-8
ASD(PA) prepublication review . . . . . Exh 8B
NAVY IPO approval . . . . . 8-8
Symposium and presentations . . . . . Exh 8B
PRESIDENT (U.S.) . . . . . 1-3, 4-20, 4-24
PRIVACY ACT (PA) . . . . . 4-11, 12-12
PROCEDURES FOR ASSIGNING DISTRIBUTION STATEMENTS ON
TECHNICAL DOCUMENTS . . . . . Exh 8A
PROCUREMENT OF NEW SECURITY EQUIPMENT . . . . . 10-4
PROGRAM PROTECTION PLAN (PPP) . . . . . 11-1
PROGRAM REVIEWS . . . . . 2-11
PROPRIETARY INFORMATION (PROPIN) . . . . . 4-16, 6-12, 11-13
PUBLIC MEDIA COMPROMISES . . . . . 12-18
PUBLIC RELEASE (See PREPUBLICATION RELEASE)

R

RANKIN PROGRAM . . . . . 5-3
RECEIPTS (classified) . . . . . 9-10
RECORD OF RECEIPT . . . . . Exh 9B
RECORDINGS . . . . . 6-31
RECOVERY OF CLASSIFIED INFORMATION . . . . . 12-6
REGISTERED MAIL . . . . . 9-3, 9-4, 9-9
REMARKING
Upgraded, downgraded or declassified documents . . . . . 6-22
REMOVABLE AIS STORAGE MEDIA . . . . . 6-33
REMOVAL OF CLASSIFIED INFORMATION FROM DESIGNATED
OFFICE OR WORKING SPACES . . . . . 10-10
REMOVAL OF SECURITY CONTAINERS . . . . . 10-5
REPAIR OF SECURITY CONTAINERS . . . . . 10-15
REPLACEMENT OF COMBINATION LOCKS . . . . . 10-11
REPORT CONTROL SYMBOLS . . . . . 2-13, App C
REPRODUCTION CONTROLS . . . . . 7-13
RESIDENTIAL STORAGE . . . . . 10-10
RESOLUTION OF CONFLICTS BETWEEN OCAs . . . . . 4-13
RESTRICTED DATA (RD) . . . . . 1-1
Dissemination . . . . . 8-4
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5

R

"RESTRICTED" FOREIGN GOVERNMENT INFORMATION . . . . . 4-17
  Marking . . . . . 6-5, 6-11
REVIEW AND CLEARANCE BY THE ASD(PA) PRIOR TO PUBLIC
  RELEASE . . . . . Exh 8B
REVIEWS
  OCAs . . . . . 12-15, 12-17
  Superiors . . . . . 12-14

S

SAFEGUARDING . . . . . 7-1
  Alternative or compensatory control measures . . . . . 7-8
  Control measures . . . . . 7-2
  During classified meetings . . . . . 7-12
  During visits . . . . . 7-11
  During working hours . . . . . 7-9
  Foreign Government Information (FGI) . . . . . 7-7
  Foreign Government "RESTRICTED" and unclassified
    information provided in confidence . . . . . 4-17, 7-7
  Safe combinations . . . . . 10-12
  Secret and Confidential information . . . . . 7-4
  Special types of classified and controlled unclassified
    information . . . . . 7-7
  Top Secret information . . . . . 7-3
  U.S. classified information located in foreign
    countries . . . . . 10-21
  Working papers . . . . . 7-6
SAMPLE
  PI letter format . . . . . Exh 12A
  PI message format . . . . . Exh 12B
  JAGMAN appointment letter . . . . . Exh 12C
  JAGMAN investigation format . . . . . Exh 12D
SCHEMATICS . . . . . 6-27
SECRETARY OF THE NAVY (SECNAV) . . . . . 1-5
SECRET INFORMATION
  Destruction . . . . . 10-19
  Dissemination . . . . . 8-3
  Records of receipt . . . . . 10-19
  Safeguarding . . . . . 7-4
  Transmission/transportation . . . . . 9-3
  OCA . . . . . 4-4
SECURE ROOMS . . . . . 10-7
  Construction standards . . . . . Exh 10A
  Priority for replacement . . . . . Exh 10B
SECURING SECURITY CONTAINERS . . . . . 10-14
SECURITY
  Action Hotline . . . . . 1-2
  Assistants . . . . . 2-4

SECURITY (Con't)
Containers (see SECURITY CONTAINERS)
End of day checks . . . . . 7-10
SECURITY CLASSIFICATION GUIDES (SCGs)
Categories . . . . . 5-3
Index of . . . . . 5-3
Multi-service/interest in . . . . . 5-5
Preparation of . . . . . 5-2
RANKIN . . . . . 5-3
Requirements for . . . . . 5-1
Reviews by OCAs . . . . . 5-4
SECURITY CONTAINERS . . . . . Exh 1A
Combinations . . . . . 10-12
Forms . . . . . 10-12
Maintenance record . . . . . Exh 10C
Priority for replacement . . . . . Exh 10B
Procurement . . . . . 10-4
Removal . . . . . 10-5
Shipboard . . . . . 10-6
Specialized . . . . . 10-8
SECURITY DISCREPANCIES INVOLVING IMPROPER
TRANSMISSIONS . . . . . 12-19
SECURITY DISCREPANCY NOTICE . . . . . Exh 12E
SECURITY EDUCATION (Information security)
Special requirements . . . . . 3-3
SECURITY INSPECTION CHECKLIST . . . . . Exh 2C
SECURITY MANAGER . . . . . 2-1
SECURITY OFFICER . . . . . 2-9
SECURITY POLICY BOARD (SPB) . . . . . 1-3
SECURITY SERVICING AGREEMENTS (SSAs) . . . . . 2-10
SENIOR OFFICIAL OF THE INTELLIGENCE COMMUNITY (SOIC) . . . . 1-4
SENSITIVE INFORMATION (COMPUTER SECURITY ACT OF 1987) . . . 1-1
Destruction . . . . . 10-20
Dissemination . . . . . 8-4
Loss or compromise . . . . . 12-8
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
SENSITIVE COMPARTMENTED INFORMATION (SCI) . . . . . 1-5
Destruction . . . . . 10-17
Dissemination . . . . . 8-4
Marking . . . . . 6-12
Loss or compromise . . . . . 12-8
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs) . . . 2-8
SHIPBOARD CONTAINERS . . . . . 10-6

SHIPMENTS
Classified bulky material . . . . . 9-7
SHREDDERS . . . . . 10-18
SINGLE INTEGRATED OPERATIONAL PROGRAM (SIOP)/SINGLE INTEGRATED OPERATIONAL PROGRAM - EXTREMELY SENSITIVE INFORMATION (SIOP-ESI) . . . . . 1-5
Destruction . . . . . 10-17
Dissemination . . . . . 8-4
Loss or compromise . . . . . 12-8
Marking . . . . . 6-11
Safeguarding . . . . . 7-7
Transmission/transportation . . . . . 9-5
SLIDES . . . . . 6-29
SOUND RECORDINGS . . . . . 6-31
SPECIAL ACCESS PROGRAMS (SAPs) . . . . . 1-1
Dissemination . . . . . 8-4
Loss or compromise . . . . . 7-7
Safeguarding . . . . . 9-5
Transmission/transportation . . . . . 12-8
SPECIAL ASSISTANT FOR NAVAL INVESTIGATIVE MATTERS AND SECURITY . . . . . 1-5
SPECIAL NATIONAL INTELLIGENCE ESTIMATES (SNIEs) . . . . . 11-14
SPECIALIZED SECURITY CONTAINERS (See CONTAINERS)
SPECIAL SECURITY OFFICER (SSO)
Designation . . . . . 2-8
For Marine Corps . . . . . 1-5
For NAVSECGRU . . . . . 1-5
SSO NAVY (ONI-5) . . . . . 1-5, 2-8
STANDARD FORMS (SFs) . . . . . App B
STORAGE . . . . . 10-1
Areas for bulky Secret and Confidential material . . . . 10-3
Cabinets . . . . . 10-6
Confidential . . . . . 10-3
Containers . . . . . 10-5, 10-6, 10-9, 10-14
Equipment . . . . . 10-2, 10-4
Requirements . . . . . 10-3
Residential . . . . . 10-10
Secret . . . . . 10-3
Standards . . . . . 10-2
Top Secret . . . . . 10-3
STORAGE EQUIPMENT . . . . . 10-2
STORAGE REQUIREMENTS . . . . . 10-3
SUBJECT AND TITLES . . . . . 6-6
SYSTEMATIC DECLASSIFICATION REVIEWS . . . . . 4-22
TECHNICAL DOCUMENTS
Dissemination . . . . . 8-7
Distribution statements . . . . . Exh 8A

T

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) . . . . . 7-12
TELEPHONE TRANSMISSION . . . . . 9-6
TENTATIVE CLASSIFICATION . . . . . 4-14
TEST CERTIFICATION LABEL . . . . . 10-4
"THIRD AGENCY RULE". . . . . 8-5
TOP SECRET . . . . . 4-2
  Destruction . . . . . 10-19
  Dissemination . . . . . 8-2
  Inventory . . . . . 7-3
  OCA . . . . . 4-4
  Records of receipt . . . . . 9-8
  Safeguarding . . . . . 7-3
  Transmission/Transportation . . . . . 9-2
TOP SECRET CONTROL OFFICER (TSCO) . . . . . 2-3
  Top Secret Control Assistant (TSCA). . . . . 2-4
TRAFFIC REVIEW OF COMSEC MATERIAL . . . . . 12-8
TRAINING OR TEST DOCUMENTS . . . . . 6-20
TRANSLATIONS . . . . . 6-16
TRANSMISSION/TRANSPORTATION . . . . . 9-1
  Aboard commercial aircraft . . . . . 9-13
  Bulky freight shipments . . . . . 9-7
  Classified to foreign government . . . . . Exh 9A
  Commercial carriers . . . . . Exh 9A
  Confidential . . . . . 9-4
  Contractors . . . . . 11-9
  Record of receipt . . . . . Exh 9B
  Secret . . . . . 9-3
  Special types of classified and controlled unclassified
     information . . . . . 9-5
  Through foreign postal systems . . . . . Exh 9A
  To the Senate . . . . . 9-14
  To the Congress . . . . . 8-6
  Top Secret . . . . . 9-2
TRANSMITTALS (See letters of transmittal)
TRANSPARENCIES . . . . . 6-29

U

U.S. POSTAL SERVICE
  Certified mail . . . . . 9-4
  Express Mail Service . . . . . 9-4, 9-9
  First Class mail . . . . . 9-4
  Registered mail . . . . . 9-3, 9-4
UNAUTHORIZED DISCLOSURE . . . . . 1-1, 4-2, 12-1, 12-18
UNITED STATES SECURITY AUTHORITY FOR NATO (USSAN). . . . . 1-4
UNPROCESSED FILM . . . . . 6-28

U

UPGRADING, DOWNGRADING OR DECLASSIFIED DOCUMENTS
Marking . . . . . 6-22
Notification of . . . . . 6-22

V

VAULTS . . . . . 10-3, 10-7
Construction standards . . . . . 10-2
Maintenance record . . . . . Exh 10C
Priority for replacement . . . . . Exh 10B
VIDEO TAPES . . . . . 6-30
VISIT BY CLEARED DoD CONTRACTOR EMPLOYEES . . . . . 11-10

W

WAIVERS . . . . . 1-2, 6-5
WARNING NOTICES . . . . . 6-11
WASTE (Classified) . . . . . 7-9, 10-19
WORKING PAPERS (Classified) . . . . . 7-6