THE SECRETARY OF THE NAVY

SECNAV M-5510.36
JUNE 2006

DEPARTMENT OF THE NAVY

INFORMATION SECURITY PROGRAM




PUBLISHED BY
CHIEF OF NAVAL OPERATIONS (N09N)
SPECIAL ASSISTANT FOR NAVAL INVESTIGATIVE MATTERS
AND SECURITY

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL OPERATIONS (N09N2)
INFORMATION AND PERSONNEL SECURITY
WASHINGTON NAVY YARD DC 20388-5380

30 June 2006

FOREWORD

The Department of Navy (DON) Information Security Program (ISP) establishes uniform policies and procedures for classifying, safeguarding, and declassifying national security information (NSI); implements Executive Order (EO) 12958, as Amended, "Classified National Security Information" and EO 12829, "The National Industrial Security Program"; and incorporates information security polices and procedures established by other executive branch agencies.

This Manual establishes specific policy set forth in SECNAVINST 5510.36A, "Department of Navy (DON) Information Security Program (ISP) Instruction." It is intended to provide uniform implementation of ISP policy and procedures throughout the DON. It encompasses all NSI classified under EO 12958, as Amended, and predecessor orders, and special types of classified and controlled unclassified information. It applies to all DON commands and to all DON military and civilian personnel.

This Manual should be read in its entirety. Major changes to the DON ISP include new policies established by EO 12958, as Amended; new classification marking guidance issued by the Office of the Under Secretary of Defense (Intelligence) to enhance information sharing efforts; revised DoD policy on Alternative Compensatory Control Measures; organizational changes to DoD and DON information security program management; guidance for classified information processed or compromised on information technology systems; and changes to industrial security requirements resulting from changes in operational support at the Defense Security Service.

DON commanding officers shall establish and conduct an ISP in compliance with this Manual and SECNAVINST 5510.36A. Questions regarding DON implementation shall be referred to CNO (N09N).

This manual may be accessed through the Department of Navy, Navy Electronics Directives System website: http://neds.daps.dla.mil.

Thomas A. Betro
Special Assistant for Naval
Investigative Matters and Security

TABLE OF CONTENTS

Chapter 7: Safeguarding

Chapter 10: Storage and Destruction

Chapter 11: Industrial Security Program

Chapter 12: Loss or Compromise of Classified Information

APPENDICES

CHAPTER 1

INTRODUCTION TO THE INFORMATION SECURITY PROGRAM

1-1 PURPOSE, APPLICABILITY, AND SCOPE

1. **Purpose**

a. This policy manual 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 policy manual also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this policy manual to describe classified material in any matter, document, product, or substance on or in which classified information is recorded or embodied, including that classified information that resides on classified Information Technology (IT) systems.

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

2. **Applicability**

a. This policy manual applies to all personnel, military and civilian, assigned to or employed by any element of the DON, and includes cleared contractor visitors working under the purview of a commanding officer. Personnel are individually responsible for compliance. This policy manual establishes the minimum standards for classifying, safeguarding, transmitting and destroying classified information as required by higher authority.

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

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

3. **Scope**. This policy manual 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 policy manual 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).

1-2 NATIONAL AUTHORITIES FOR SECURITY MATTERS

1. **The President** of the United States (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 classifying, safeguarding, downgrading, and declassifying classified national security information in reference (a).

2. **The National Security Council (NSC)** provides overall policy guidance on information 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). Reference (b) establishes national standards for the classification and marking of classified national security information, security education and training programs, self-inspection programs, and declassification. The ISOO is responsible for overseeing 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 Chief of Naval Operations (CNO)(N09N2)).

4. **The Director of Central Intelligence (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 prescribes measures for protecting intelligence sources and methods via reference (f).

5. **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.

1-3 DOD SECURITY PROGRAM MANAGEMENT

1. **The Under Secretary of Defense (Intelligence) (USD(I))** is the Department of Defense (DoD) senior official charged by the Secretary of Defense (SECDEF) with responsibility for developing policies and procedures governing information and personnel security, including atomic energy policy programs.

2. **The Deputy Under Secretary of Defense ((Communications, Intelligence and Security) (ODUSD (CI&S))** produces references (c) and (d). Reference (d) is the primary source for the policies and procedures in this policy manual.

3. **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 Special Access Programs (SAP), the National Disclosure Policy (NDP), Foreign Government Information (FGI) (including North Atlantic Treaty Organization (NATO) information), and security arrangements for international programs.

4. **The Deputy Under Secretary of Defense (Technology Security Policy and National Disclosure Policy) (ODUSD (TSP&NDP))** 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.

5. **The National Security Agency (NSA)** provides centralized coordination and direction for signals intelligence and communications security for the U.S. Government. The Director, NSA is authorized by the SECDEF to prescribe procedures or requirements, in addition to those in DoD instructions, for COMSEC. The authority to lower any COMSEC security standards within the DoD rests with the SECDEF.

6. **The Defense Intelligence Agency (DIA)** is responsible for the direction and control of SCI programs established by DOD components.

1-4 DON SECURITY PROGRAM MANAGEMENT

1. **The Secretary of the Navy (SECNAV)** is responsible for implementing an ISP per the provisions of Executive Orders (EO), public laws, and directives issued by the NSC, Department of Energy (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)** is designated by the SECNAV as the DON senior agency official under reference (a) and the DON Restricted Data (RD) management official under reference (g).

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 the National Industrial Security Program within the DON.

(3) Ensuring that persons with access to RD (including Critical Nuclear Weapons Design Information (CNWDI)) and Formerly Restricted Data (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, Office of the SECDEF and other DoD components and Federal agencies.

(5) Maintaining a world wide web page that provides information related to the DON Information and Personnel Security Program (PSP). The Web page may be found at www.navysecurity.navy.mil.

b. The CNO (N09N) is also responsible for establishing, administering, and overseeing the DON PSP, and issuing personnel security policy and procedures in reference (h).

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 Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director for Information and Personnel Security Programs (NCIS-24E)** provides staff support for the CNO (N09N) functions and responsibilities described in paragraph 2.

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 national disclosure policy and manages certain personnel exchange programs with foreign governments.

5. **The Director of Naval Intelligence (DNI) (CNO (N2))** is a Senior Official of the Intelligence Community (SOIC) and administers the SCI program for the Navy, including non-Service DON entities.

6. **The Director of Intelligence of the Marine Corps** is a Senior Official of the Intelligence Community (SOIC) and administers the SCI program for the Marine Corps.

7. **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 (j), (k), and (l).

8. **The Department of the Navy, Chief Information Officer (CIO)** is responsible for DON policies and implementation of the DoD IA program under references (m) and (n), respectively. The DON CIO issues reference (o), and is also responsible for Information Management and Information Management Resource Technology matters.

9. **The Assistant Chief of Naval Operations, Information Technology (ACNO (IT), (N098)),** in coordination with the DON CIO, is responsible for policy, implementation, and oversight of the DON IA program in accordance with reference (o).

10. **The Naval Network Warfare Command (NETWARCOM):**

a. **The Commander, NETWARCOM** is responsible for implementing the DON CIO policies within the DON.

b. **The NETWARCOM Security Directorate,** as the designated SSO for the Commander, NETWARCOM, is responsible for signals intelligence activities and for administration of SCI programs within the DON cryptologic community.

11. **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 reference (p).

12. **The Commandant of the Marine Corps (CMC)** administers the DON ISP within the U.S. 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 and the ISP. All requirements for policy waivers, interpretations and exceptions will be reviewed by the CMC (Code ARS).

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

1-5 POLICY GUIDANCE

1. **Assistance Via the Chain of Command**. DON personnel are encouraged to obtain guidance or interpretation of policy and procedures in this policy manual via the chain of command.

2. Telephone inquiries may be made to the CNO (N09N2) **Security Action Hotline** at (202) 433-8856. After hours calls are recorded and returned as soon as possible. Additional information may be obtained at the CNO (N09N2) web page at **www.navysecurity.navy.mil**.

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

4. **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 policy manual, 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, consecutively assigned number, and the year (e.g., N12345-E(I)-01-05) to each waiver or exception request. Include a point of contact and telephone number with the request. Waivers and exceptions are self-cancelling at the end of the specified period, 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 policy manual.

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

5. **Alternative Compensatory Control Measures (ACCM)**. Reference (d) authorizes the DON to employ alternative compensatory security controls for safeguarding classified information.

Procedures for submitting requests and requirements for approval are contained in chapter 7, paragraph 7-9.

1-6 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. **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 reference (p).

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

c. **Special Access Programs (SAPs)**. All SAPs must be authorized by the SECDEF or the Deputy SECDEF and are governed by references (j) through (l). The Under Secretary of the Navy must formally approve the establishment of each SAP in coordination with the Deputy SECDEF. The Director, Special Programs Division (N7SP), coordinates all requests for SAPs.

d. **Single Integrated Operational Plan (SIOP) and Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)**. SIOP and SIOP-ESI are governed by reference (q), which is issued by the CNO (N5 GP).

e. **Naval Nuclear Propulsion Information (NNPI)**. Classified and unclassified NNPI is governed by reference (r).

f. **Restricted Data (RD) and Formerly Restricted Data (FRD)**. RD and FRD are governed by reference (s) and the Department of Energy (DOE) Regulations implemented by reference (t). Access to **Critical Nuclear Weapons Design Information (CNWDI),** a special category of RD, is also governed by reference (t).

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 U.S. and the foreign entity.

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

2. **Controlled Unclassified Information (CUI).** CUI is defined and governed by laws, international agreements, EOs, and regulations that address the identification, marking, protection, handling, transmission, transportation, and destruction. Categories of Controlled Unclassified Information include:

a. For Official Use Only (FOUO) information, as defined under the Freedom of Information Act (FOIA) (reference (v); protective measures as prescribed by reference (d)); Law Enforcement Sensitive Information (LES) (reference (d);

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

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

d. Drug Enforcement Administration (DEA) Sensitive Information (reference (d));

e. Unclassified information in technical documents requiring distribution statements (reference (x)); and

f. National Geospatial Intelligence Agency Limited Distribution Information (reference (y)).

1-7 NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

The NISP was established by reference (e) 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 executive branch departments and agencies. The NISP applies to information classified under references (a) and (s).

REFERENCES

(a) Executive Order 12958, as Amended, *Classified National Security Information*, 25 Mar 03

(b) 32 CFR Parts 2001 and 2004, *Classified National Security Information (ISOO Directive No. 1)*, 22 Sep 03

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

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

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

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

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

(h) SECNAVINST 5510.30B, *DON Personnel Security Program Regulation*

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

(j) DoD Directive 5205.7, *Special Access Program (SAP) Policy*, 5 Jan 06

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

(l) SECNAVINST S5460.3C, *Management, Administrative Support and Oversight of Special Access Programs Within the Department of the Navy (U)*, 5 Aug 99

(m) DoD Directive 8500.1, *Information Assurance (IA)*, 24 Oct 02

(n) DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 03

(o) SECNAV M-5239.1, *Department of the Navy Information Assurance (IA) Program*, Nov 05

(p) *EKMS-1, CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

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

(r) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI)*, 26 Jul 05

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

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

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

(v) Title 5, U.S.C., Section 552, *Freedom of Information Act of 4 Jul 66, as amended*

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

(x) DoD Directive 5230.24, *Distribution Statements on Technical Documents,* 18 Mar 87

(y) DoD Directive 5030.59, *National Imagery and Mapping Agency (NIMA) Limited Distribution Imagery or Geospatial Information and Data,* 13 May 03

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 policy manual 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 policy manual to a commanding officer may be further delegated unless specifically prohibited.

3. **Standards.** This policy manual 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 policy manual 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 that 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 perform classified work or operate within areas under the direct control of the commanding officer.

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

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 policy manual. 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 policy manual are immediately referred to the nearest NCIS office.

f. Ensure that all security violations or incidents involving the possible compromise of classified information, to include those involving information technology (IT) systems, are investigated and reported in accordance with chapter 12 of this policy manual. Coordinate after-incident responses involving classified information processed on IT systems with the command Information Assurance Manager (IAM).

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

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

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

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

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

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

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

n. 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 five years prior to assignment.

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. Top Secret Control Assistants (TSCA) may be assigned as needed (see paragraph 2-4.3). 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, or more frequently when circumstances warrant (see chapter 7, paragraph 7-3). As an exception, repositories, libraries, or activities that store large volumes of classified documents may limit their annual inventory to that which access has been given in the past 12 months, and 10 percent of the remaining inventory.

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 a favorably adjudicated SSBI within the previous five years.

3. Commands may designate more than one TSCO when circumstances warrant and the duties of each can easily be delineated, such as for commands that maintain separate and distinct program-specific libraries or repositories.

2-4 OTHER SECURITY ASSISTANTS

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

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

3. **Top Secret Control Assistant (TSCA)**. Individuals may be assigned to assist the TSCO as needed. The designation must be in writing. A person designated as a TSCA must be a U.S. citizen, and have a favorably adjudicated SSBI within the

previous five years. An established Top Secret security clearance eligibility is required. Top Secret couriers are not considered to be TSCAs.

2-5 SECURITY RELATED COLLATERAL DUTIES

1. **Electronic Key Management System (EKMS) Manager**. The commanding officer must designate, in writing, an EKMS Manager. The EKMS manager is the principal advisor to the commanding officer in all matters regarding the Communication Material System (CMS). Specific selection and other designation requirements for an EKMS manager and alternate are outlined in reference (d).

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 will exercise control over receipt, correction, stowage, security, accounting, distribution, and authorized destruction of all NWPs. The NWP custodian will ensure, in coordination with the command security manager, completion of Preliminary Inquiries (PIs) and Judge Advocate General Manual (JAGMAN) investigations for loss or compromised publications in accordance with chapter 12 of this policy manual.

3. **North Atlantic Treaty Organization (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 Central United States Registry (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 sub-registries 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. The designation shall be for the purpose of preparing and signing the “Contract Security Classification Specification” (DD Form 254), and revisions thereto, and other

security related contract correspondence. 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 ASSURANCE MANAGER (IAM)

Per reference (h), the commanding officer shall designate, in writing, an IAM and Information Assurance Officer(s) (IAO), as appropriate. The IAM was previously called the "Information Systems Security Manager (ISSM)," and the IAO was previously called the "Information Systems Security Officer (ISSO)." The IAM serves as the point of contact for all command information assurance (IA) matters and implements the command's IA program. IAOs are designated for each information system and network in the command, and are responsible for implementing and maintaining the command's information technology systems and network security requirements.

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, Office of Naval Intelligence (ONI) or Commander, Naval Network Warfare Command (COMNAVNETWARCOM) Security Directorate.

2. The SSO and the SSSO shall be appointed in writing and each 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, or Memoranda of Understanding (MOU) or Memoranda of Agreement (MOA). 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 for 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. 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 that may directly affect the security integrity of the command.

2-11 INSPECTIONS, ASSIST VISITS, AND PROGRAM REVIEWS

1. Commanding officers are responsible for evaluating and documenting the security posture of the command and subordinate commands. These self-inspections may be conducted using the format suggested in exhibit 2C, or they may focus on one functional area or discipline.

2. It is not necessary to conduct separate inspections for security, unless otherwise required. 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 Personnel Security Program (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 policy manual.

REFERENCES

(a) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 Feb 06

(b) SECNAVINST 5510.30 (Series), *DON Personnel Security Program Instruction*

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

(d) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

(e) NTTP 1-01, *Naval Warfare Library,* Apr 05

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

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

(h) OPNAVINST 5239.1B, *Navy Information Assurance (IA) Program,* 9 Nov 99

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

(j) DCID 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, 2 Jul 98

(k) OPNAVINST 5530.14C, *Navy Physical Security*, 10 Dec 98

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 policy manual and identify any unique command requirements. The command security instruction shall supplement this policy manual and other directives from authorities in the command administrative and operational chain, and should be signed by the Commanding Officer.

2. The command security instruction shall:

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

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Cite and append Security Service Agreements (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 counterintelligence matters to the nearest NCIS office.

h. Establish 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 original classification authority.

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

k. Establish an industrial security program and identify key personnel, such as the 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; safeguarding of U.S. classified information located in foreign countries; identifying Information Technology systems processing classified information; and describing any authorized residential storage arrangements.

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

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

3. Refer to SECNAVINST 5510.30B 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 (EKMS-1 provides additional emergency destruction policy and guidance for commands that handle COMSEC information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of emergency destruction of classified information 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 Information Technology 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 5510.36A? (1-1)

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

__ __ __ a. COMSEC, EKMS-1?
__ __ __ b. DoD SCI Security Manual/relevant DCIDs?
__ __ __ c SAPs, OPNAVINST S5460.3C?
__ __ __ d. SIOP and SIOP-ESI, OPNAVINST S5511.35K?
__ __ __ e. NNPI, NAVSEAINST 5511.32C?
__ __ __ f. RD/FRD, DoD Directive 5210.2?
__ __ __ g. CNWDI, DoD Directive 5210.2?
__ __ __ h. Classified information released to industry, DoD 5220.22-R?

__ __ __ 3. Are waivers and exceptions submitted to the CNO (N09N2) for all conditions that prevent compliance with SECNAVINST 5510.36A? (1-5)

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. EKMS manager 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 public 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 (to include subordinate commands)? (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 and their officially "Acting" alternates?
__	__	__	b. Derivative classifiers, security managers, and other security personnel?
__	__	__	c. Classified couriers?
__	__	__	d. Declassification authorities?

CLASSIFICATION MANAGEMENT

__	__	__	1. Is information classified only to protect the national security? (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 OCA training (i.e., indoctrination letter) been submitted to the CNO (N09N2)? (4-6)
__	__	__	5. Is information that has been released to the public without proper authority classified or reclassified only when the information can be reasonably recovered, most individual

YES	NO	N/A		
				holders are known, and is it withdrawn from public access? (4-11)
__	__	__	6.	Is the classification level of any information, believed to be improperly classified, challenged? (4-12)
__	__	__	7.	Do NATO and FGI retain the original classification level and assigned a U.S. classification equivalent, if necessary? (4-17, 6-16)
__	__	__	8.	Are procedures established for initial response to command mandatory declassification reviews within 45 working days? (4-22)
__	__	__	9.	Are reasonable steps taken to declassify information determined to be of permanent historical value prior to its accession into NARA? (4-24)
__	__	__	10.	Have cognizant OCAs notified holders of unscheduled classification changes involving their information? (4-25)

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 5513.1F? (5-2)
__	__	__	4.	Are command-originated SCGs reviewed, by the cognizant OCA, at least every 5 years? (5-4)

YES	NO	N/A		
__	__	__	5.	Are all changes promptly submitted to the RANKIN Program Manager (CNO (N09N2))? (5-4)

MARKING

__	__	__	1.	Are classified documents and their portions properly marked to include all applicable basic and associated markings? (6-1, 6-7)
__	__	__	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 applicable 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? (6-16)
__	__	__	10.	Is the face of NATO and foreign government RESTRICTED documents and FGI marked with the appropriate notice? (6-16)

YES	NO	N/A		
__	__	__	11.	Is the assignment and use of nicknames, exercise terms, and code words per OPNAVINST 5511.37C? (6-18)
__	__	__	12.	Is an explanatory statement included on the face of documents classified by compilation? (6-19)
__	__	__	13.	Do documents, marked classified for training and test purposes, include a statement indicating that the documents are actually unclassified? (6-21)
__	__	__	14.	When removed or used separately, are component parts of classified documents marked as separate documents? (6-22)
__	__	__	15.	Are letters of transmittal marked to show the highest overall classification level of any information being attached or enclosed? (6-25)
__	__	__	16.	Are electronically transmitted messages properly marked? (6-26)
__	__	__	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? (6-27)
__	__	__	18.	Are all classified materials such as IT media, maps, charts, graphs, photographs, briefing slides, recordings, and videotapes appropriately marked? (6-28 through 6-35)
__	__	__	19.	Are classified emails sent over secure IT systems marked as required? (6-35)

SAFEGUARDING

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

YES	NO	N/A		
				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)
__	__	__	5.	Are control measures in place to protect unauthorized access to command TS, Secret, 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. Controlled and marked after 180 days or when they are released outside the command?
__	__	__	7.	Are appropriate control measures taken for other special types of classified information? (7-8)
__	__	__	8.	Are SFs 703, 704, and 705 placed on all classified information when removed from secure storage? (7-10)
__	__	__		a. Are SFs 706, 707, 708, and 712 being utilized on classified IT system media, when feasible?
__	__	__		b. When SF media labels are not feasible due to the size of the media or

YES	NO	N/A		
				interference with media operation, are other methods for identifying the classification of the media used?
__	__	__	c.	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? (7-11)
__	__	__	10.	Are classified vaults, secure rooms, and containers made an integral part of the end of day security check? (7-11)
__	__	__	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 eligibility? (7-12)
__	__	__	12.	Are procedures in place for classified meetings held at the command or hosted at cleared facilities? (7-13)
__	__	__	13.	Is classified information reproduced only to the extent that it is mission essential? (7-15)

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 5730.5G and OPNAVINST 5510.158A? (8-6)

YES	NO	N/A	
__	__	__	4. Do all newly generated classified and unclassified technical documents include a distribution statement listed in **exhibit 8A** of SECNAVINST 5510.36A? (8-7)
__	__	__	5. Is unclassified technical data which reveals critical technology with military or space application and requires an approval, authorization, or license for its lawful export withheld from public disclosure per OPNAVINST 5510.161? (8-7)
__	__	__	6. Is command information intended for public release, including information released through IT systems (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)
__	__	__	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

YES	NO	N/A	
			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 (N3AT)? (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?
__	__	__	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, registered mail and commercial express deliveries 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)

YES	NO	N/A		
__	__	__	6.	Are specialized security containers securely fastened to the structure, rendering them non-portable? (10-8)
__	__	__	7.	Has the command disposed all containers manufactured by Remington Rand and disqualified containers manufactured by Art Metal? (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 container has been subjected to compromise?
__	__	__		e. Whenever the container is taken out of service?
__	__	__	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 the persons to be contacted if the container is found opened and unattended? (10-12)

YES	NO	N/A		
__	__	__	13.	Is the combination placed in the SF 700, and is it properly secured in an appropriate security container? (10-12)
__	__	__	14.	Has the command established procedures for command key and padlock accountability and control? (10-13)
__	__	__	15.	Are command locks repaired only by authorized personnel who have been subject to a trustworthiness determination or who are continuously escorted? (10-15)
__	__	__	16.	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)
__	__	__	17.	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)
__	__	__	18.	Are all commercial IDSs used on command security containers, vaults, modular vaults, and secure rooms approved by the CNO (N3AT)? (10-16)
__	__	__	19.	Is command classified information destroyed when no longer required? (10-17)
__	__	__	20.	Do all command shredders, pulverizers, and disintegrators meet the minimum requirements? (10-18)
__	__	__	21.	Is the command replacing old shredders or those that need repair with shredders that meet the new NSA Standards? (10-18)
__	__	__	22.	Has the command established effective procedures for the destruction of classified information? (10-19)

YES NO N/A

__ __ __ 23. When filled, are command burn bags sealed and safeguarded per the highest overall classification level of their contents? (10-19)

__ __ __ 24. 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 imposed any PPPs on its contractors via the contract? (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? (11-4)

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

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

YES	NO	N/A	
__	__	__	5. Have all FADs been issued per SECNAVINST 5510.30B? (11-7)
__	__	__	6. Is classified intelligence information disclosed only to those contractors cleared under the NISP and as authorized on the DD 254? (11-13)

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

__	__	__	1. Is the command security manager responsible for overseeing the response to all losses or compromises of classified information, including those that occurred on IT systems? (12-2)
			2. Since the last inspection, has the command had any incidents involving a loss or compromise of classified information? (12-1)
__	__	__	3. If a possible loss or compromise occurred, was a PI conducted and documented? (12-4)
__	__	__	4. If a significant command weakness is identified, if disciplinary action is contemplated, or a confirmed or probable loss or compromise occurred, was a JAGMAN investigation conducted? (12-7 and 12-9)
__	__	__	5. Were all appropriate parties, to include the originator of the information, the OCA, other DOD or federal agencies, notified of the compromise as part of the PI and JAGMAN? (12-4 and 12-13)
__	__	__	6. 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)

YES	NO	N/A	
__	__	__	7. Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent compromise or repeated administrative disregard of security regulations occurs? (12-14)
__	__	__	8. Are procedures established for review of investigations by seniors? (12-14)
__	__	__	9. Are security reviews conducted on information subjected to loss or compromise? (12-15)
__	__	__	10. Are procedures established for classification reviews by originators or OCAs? (12-16)
__	__	__	11. 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 ensure proper execution of their security responsibilities.

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) and officials acting in their absence, on an annual basis (see chapter 4, paragraph 4-6);

    b. Derivative classifiers (see chapter 4, paragraph 4-9), security managers, 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 5510.30 (Series), *DON Personnel Security Program Instruction*

CHAPTER 4

CLASSIFICATION MANAGEMENT

4-1 BASIC POLICY

1. Reference (a) is the only basis for classifying national security information, 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) shall be codified in security classification guides, and it shall be declassified as soon as it no longer meets the standards for classification in the interest of the national security. Exhibit 4A lists current DON OCAs, and updates to this list can be found at www.navysecurity.navy.mil.

4-2 CLASSIFICATION LEVELS

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

3. **Secret** is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **serious damage** to the 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.

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

1. 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 codify original classification decisions in Security Classification Guides (see chapter 5).

2. OCAs are designated by virtue of their position. Original classification authority is not transferable. In instances where the OCA is absent for extended periods of time and an emergent need requires that the authority be exercised prior to the OCA's return, it may be judiciously exercised by an individual officially designated to act in the OCA's absence.

3. Indoctrination training in paragraph 4-6 must be accomplished prior to exercising the authority. Both the OCA and any individual officially acting in his OCA capacity as described in paragraph 4-4.2 must receive this training. OCA's and acting OCAs must have annual refresher training on OCA duties and responsibilities.

4. Only the incumbents of the positions listed in exhibit 4A have original classification authority. Periodic updates to exhibit 4A can be found at www.navysecurity.navy.mil.

4-5 REQUESTS FOR ORIGINAL CLASSIFICATION AUTHORITY

1. Requests for Top Secret original classification authority shall be submitted, in writing, to the Secretary of the Navy via CNO (N09N2). Requests for Secret or Confidential original classification authority shall be submitted, in writing, directly 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, and the individual officially designated to act in their absence, 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. Training shall consist of a review of the pertinent EO, statutes, and DON regulations which can be found on the CNO (N09N2) website at www.navysecurity.navy.mil. OCAs and an individual designated to act in their absence shall provide written confirmation (i.e., indoctrination letter) to the CNO (N09N2) that this training has been accomplished. OCAs and an individual designated to act in their absence must also have annual refresher training on these responsibilities. For continuity, this refresher training may be given in conjunction with other command annual security training requirements described in reference (c).

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 (d) contains the specific criteria, principles, and considerations for original classification. DON OCAs shall codify original classification decisions in security classification guides (see chapter 5).

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 25 years from the date of the original classification.

2. OCAs may specify duration of classification beyond 25 years only when originally classifying information that could be expected to reveal the identity of a confidential human source or human intelligence source. Only OCAs with jurisdiction over such information may originally classify information using the “25X1-human” exemption.

3. If information has been assigned a date or event for declassification that is less than 25 years, but the cognizant OCA later has reason to believe longer protection is required (i.e., program changes), the OCA may extend duration of classification up to 25 years. OCAs shall consider their ability and responsibility to notify all holders of this classification extension, before extending classification.

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.

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; and

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 and for applying proper classification markings. Officials with signature authority are also responsible for these decisions when exercising command signature authority. Security Managers may provide advice and assistance to classifiers in assigning classification for original and derivative classification decisions.

4-11 LIMITATIONS ON CLASSIFYING OR RECLASSIFYING

1. 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 (e) (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.

2. Classified information that has been released to the public without proper authority may remain classified if the cognizant OCA makes such a determination. The OCA shall notify authorized holders, and apply the following marking instructions in the event the information is not already marked:

a. Overall level of classification;

b. New portion markings;

c. Identity, by name or personal identifier and position, of the OCA;

d. Declassification instructions;

e. Concise reason for classification; and

f. Date the action was taken.

3. Information that has been declassified and released to the public under proper authority (i.e., publicly released in accordance with reference (f)) may be reclassified only under the circumstances described in this section. Only the Secretary of the Navy or the Under Secretary of the Navy may reclassify the information, and this reclassification must include a written determination that reclassification is necessary in the interest of national security.

a. A cognizant OCA may request reclassification of the information, but must deem that the information can be reasonably recovered and that most individual recipients or holders are known and all forms of the information to be reclassified can be retrieved. Consideration should be given to the extent of dissemination and the practicality of retrieving the information. For example, it may not be practical to reclassify information officially released via the world wide web. If the information has been made available to the public through such means as Government archives or reading rooms, it shall be withdrawn from public access.

b. OCAs shall request reclassification, in writing, via CNO (N09N2), and shall include:

(1) A description of the information;

(2) The classification level of the information;

(3) When and how it was released to the public;

(4) An explanation of why it should remain classified, and which EO 12958, as Amended, "classification reason" applies;

(5) What damage to national security could occur and what damage may already have been done;

(6) The number of recipients/holders and how they will be notified of the reclassification action; and

(7) How the information will be recovered.

c. Cleared recipients or holders of reclassified information shall be notified within 30 days and appropriately briefed about their continuing obligation and responsibility to protect this information from unauthorized disclosure.

d. To the extent practicable, uncleared recipients of reclassified information shall be notified and appropriately briefed about the reclassification of the information and the obligation not to disclose the information. They shall also be asked to sign an acknowledgement of the briefing. Further, they shall be asked to return the information if it is in retrievable form.

4-12 CLASSIFICATION CHALLENGES

1. Authorized holders of classified information are encouraged and expected to challenge the classification of information that 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 5.3 of reference (a).

5. These procedures do not apply to or affect the mandatory declassification review actions described in paragraph 4-22.

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. Individuals, not having original classification authority, who create information they believe to be classified shall mark the information accordingly, 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.

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

3. 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 4-15 through 4-17.

2. Reference (e) 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 00) 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 to that provided by the originator to ensure adequate protection of the information (see exhibit 6C). Foreign government information retaining its original classification markings need not be

assigned a U.S. classification marking if the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

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 afforded a degree of protection that is at least equivalent to that required by the government or international organization that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including modified handling and transmission and allowing access by individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed a non-disclosure agreement. If the foreign protection requirement is lower than the protection required for U.S. Confidential, it shall be marked in accordance with chapter 6, paragraph 6-16. It may be classified at a higher level if it meets the 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 and safeguarding requirements applying to NNPI may also be found in references (h) through (k).

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 or that OCA's current successor; or

c. The next superior in the chain-of-command of paragraph 4-19(1)b, 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 cognizant OCA.

4-20 AUTOMATIC DECLASSIFICATION

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

2. Reference (a) established procedures for automatic declassification review of classified records that are more than 25 years old and have been determined to have permanent historical value as defined by reference (m). Historically valuable records are identified in reference (n) by the use of the term "permanent" in the records series disposition instruction. All 25-year old historically valuable classified records will be automatically declassified on 31 December 2006, whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on 31 December of the year that is 25 years from the date of original classification, except as provided in reference (a). If the records have been reviewed and either exempted or excluded in accordance with reference (l), or have been referred to another agency for review of that agency's equities, automatic declassification will not immediately apply.

3. Automatic declassification review of 25-year old records applies to the official records contained in the National

Archives and Records Administration (NARA) records systems. Commands holding non-record copies of classified records shall refer to reference (l) for declassification or exemption authority. If unable to make a determination, holders of 25-yearold classified information may refer the information to the current cognizant OCA for a decision, or may refer the material to CNO (N09N2) to coordinate such a decision.

4. Declassified documents will not be released to the public until a public release review has been conducted in accordance with reference (f).

4-21 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 (m).

2. The CNO (N09N) is responsible for identifying to the Archivist of the U.S. that classified DON information that is 25 years old and older which requires continued protection. This includes records of permanent historical value exempted from automatic declassification under Section 3.3 of reference (a). In coordination with the DON OCAs, the CNO (N09N) has developed reference (l) to be used by the Archivist in declassifying DON information.

3. The SECDEF may establish special procedures for systematic review for declassification of classified cryptologic information.

4. The Director, Central Intelligence (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 Restricted Data (RD) and Formerly Restricted Data (FRD) information classified per reference (b).

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

4-22 MANDATORY DECLASSIFICATION REVIEW

1. Mandatory declassification review is the review for declassification of classified information in response to a request that meets the requirements of Section 3.5 of reference (a).

2. Mandatory declassification review does not supplement or modify the procedures for the handling of FOIA requests as described in reference (o). When a requester submits a request both under mandatory review and the FOIA, the requester will be required to elect one or the other process. If the requester fails to elect a process it will be treated as a FOIA request unless the requested materials are subject only to mandatory declassification review.

3. 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 the DON to locate it with a reasonable amount of effort;

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

c. The information has not been reviewed within the preceding two years. If the information has been reviewed within the past two years, or the information is the subject of pending litigation, the requester will be informed of this fact and of the requester's 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 and the requester notified accordingly. If a declassification determination cannot be made within the 45 working days, notify the requester of the additional time needed to process the request.

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 informed of the

additional time needed to process the request. A final determination shall ordinarily be made within one year of the date of receipt.

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. When information cannot be declassified in its entirety, a reasonable effort shall be made to release those declassified portions that constitute a coherent segment. If the information is not releasable in whole or in part, the requester shall be provided a brief statement of the reason(s) for denial and notice of the right to appeal to the Interagency Security Classification Appeals Panel (ISCAP) via the CNO (N09N) within 45 working days. A final determination on the appeal shall ordinarily be made within 60 working days after receipt by the ISCAP.

d. Refer requests for declassification involving information originally classified by another agency to that agency. 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. Refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under reference (a) or its predecessors.

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

7. If withholding of the newly declassified information is authorized under other laws, the information shall be marked and safeguarded accordingly (e.g., with a technical distribution statement or FOIA exemption).

8. Mandatory declassification review should not be confused with other requests for classification or declassification review. Requests under the mandatory declassification review provisions of reference (a) must specifically refer to these provisions.

4-23 INFORMATION EXEMPTED FROM MANDATORY DECLASSIFICATION REVIEW

Information originated by the incumbent President and Vice President (in the performance of executive duties); the President's White House staff and the Vice President's staff (in the performance of executive duties); 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 (m).

4-24 CLASSIFIED INFORMATION TRANSFERRED TO THE DON

1. Classified information officially transferred to a command in conjunction with a transfer of functions, and not merely for storage purposes, shall become the possession of that command. The commanding officer of the 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 a command that has ceased to exist (and for which there is no successor command) shall become the possession of the custodial command and may be downgraded or declassified after consultation with any other command interested in the subject matter. If a determination is made that another command or outside agency may have an interest in the continued classification of the information, the custodial command shall notify the command(s) or outside agency 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 command.

3. OCAs shall take reasonable steps to declassify classified information contained in records determined to be of permanent historical value, per reference (n), before they are accessioned into the National Archives and Records Administration (NARA).

4-25 NOTIFICATION OF CLASSIFICATION CHANGES

1. OCAs are responsible for notifying holders of any classification changes involving their information. Original addressees and holders 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.

4-26 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, as Amended, *Classified National Security Information,* 25 Mar 03

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

(c) SECNAVINST 5510.30 (Series), *DON Personnel Security Program Regulation*

(d) OPNAVINST 5513.1F, *DON Security Classification Guides*, 7 Dec 05

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

(f) DoD Directive 5230.9, *Clearance of DOD Information for Public Release,* 9 Apr 96

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

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

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

(j) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 26 Jul 05

(k) NAVSEAINST 5230.12, *Release of Information to the Public,* 21 Nov 03

(l) OPNAVINST 5513.16 (Series), *Declassification of 25-Year Old DON Information*

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

(n) SECNAV M-5210.1, *Navy Records Management Program,* Dec 05

(o) SECNAVINST 5720.42F, *DON Freedom of Information Act (FOIA) Program*, 6 Jan 99

(p) Title 50, U.S.C., Subchapter V, Section 431, *Central Intelligence Agency Information Act*

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

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

EXHIBIT 4A

DEPARTMENT OF THE NAVY
ORIGINAL CLASSIFICATION AUTHORITIES

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, Strike Weapons and Unmanned Aviation (PEO-W)	TS
Program Executive Officer, Tactical Aircraft Programs (PEO-T)	TS
Program Executive Officer for Littoral and Mine Warfare (PEO-LMW)	TS
Program Executive Officer for Integrated Warfare Systems (PEO-IWS)	TS

Program Executive Officer, Command, Control, Communications, Computers and Intelligence and Space (PEO-C41 & SPACE)	TS
Program Executive Officer, Submarines (PEO-SUB)	S
Program Executive Officer Ships (PEO-SHIPS)	S
Program Executive Officer for Carriers (PEO-CARRIERS)	S

Chief of Naval Research

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

Naval Air Systems Command

Commander, Naval Air Systems Command (AIR-00)	TS
Vice Commander, Naval Air Systems Command (AIR-09)	S
Deputy Commander for Acquisition and Operations (AIR-1.0)	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	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 (05)	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

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
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
Commander, Office of Naval Intelligence, Suitland, MD (ONI-00)	TS
Deputy Chief of Naval Operations (Information, Plans and Strategy) (N3/N5)	TS
Director, Information, Plans, and Security Division (N3IPS)	TS
Director, Strategy and Policy Division (N5SP)	TS
Deputy Chief of Naval Operations (Logistics) (N4)	TS
Deputy Chief of Naval Operations Warfare Requirements and Programs (N6/N7)	TS
Director, Space, Information Warfare, Command & Control (N61)	TS
Deputy Director, Space, Information Warfare, Command and Control (N61B)	TS
Deputy Director for Warfare Capabilities, Head FORCENET Requirements (N61F)	TS
Deputy for Resources and Requirements (N61R)	S
Director, Special Programs (N7SP)	TS
Director, Expeditionary Warfare Division (N75)	TS
Head, Special Warfare Branch (N751)	S
Director, Surface Warfare Division (N76)	TS

Head, Theater Air Defense (N765)	S
Director, Submarine Warfare Division (N77)	TS
Head, Platforms, Manpower, Policy & Budget Branch (N771)	S
Head, Integration, Systems & Payloads Branch (N772)	S
Head, Undersea Surveillance (N772A)	S
Head, Deep Submergence Branch (N773)	TS
Head, Submarine Security and Technology Branch (N775)	S
Director, Air Warfare Division (N78)	TS
Head, Aviation Plans/Requirements Branch (N780)	S
Deputy Chief of Naval Operations (Resources, Warfare Requirements, and Assessments) (N8)	TS

Naval Nuclear Propulsion Program

Director, Naval Nuclear Propulsion Program (NOON)/Deputy Commander, Nuclear Propulsion Directorate, Naval Sea Systems Command (SEA-08)	TS
Deputy Director, Naval Nuclear Propulsion Program (NOONB)/Deputy Director, Nuclear Propulsion Directorate, Naval Sea Systems Command (SEA-08B)	S
Associate Director for Regulatory Affairs (N00NU)	S
Director, Nuclear Technology Division (N00NR)	S
Program Manager for Commissioned Submarines (N00N0)	S
Director, Reactor Engineering Division (N000NI)	S
Director, Submarine Systems Division (N00NE)	S

Military Sealift Command

Commander, Military Sealift Command (N00)	TS

Network Warfare Command

Commander, Naval Network Warfare Command	TS

Strategic Systems Programs

Director, Strategic Systems Programs (00)	TS

Navy International Programs Office

Director, Navy International Programs Office (00)	S

Naval Meteorology and Oceanography Command

Commander, Naval Meteorology 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, U.S. Atlantic Fleet (N00)	TS
Commander, U.S. Naval Forces, Southern Command (N2)	TS
Director of Operations, U.S. Atlantic Fleet (N3/N5)	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, U.S. Pacific Fleet (N00)	TS

U.S. Naval Forces Europe

Commander, U.S. Naval Forces Europe (N014)	TS
Deputy Commander, 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 and Information Warfare, 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, U.S. Naval Forces Central Command (00)	TS

U.S. Marine Corps

Headquarters, 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
Deputy Commandant for Plans, Policies and Operations, Marine Corps	TS
Deputy Commandant for Aviation, Marine Corps	TS
Director, Command, Control, Communications, and Computers (C4), Marine Corps	TS
Director, Intelligence Department (I), Marine Corps	S

U.S. Marine Corps Systems Command

Commander, Marine Corps Systems Command, Quantico, VA	TS

U.S. Marine Corps Fleet Commands

U.S. Marine Corps Forces, Pacific

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

U.S. Marine Corps Expeditionary Forces

Commanding General, I Marine Expeditionary Forces	S
Commanding General, III Marine Expeditionary Forces	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. Each SCG and revised SCG is considered a new original classification decision. Administrative changes where there are no changes to classification are not considered original classification decisions.

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) web page 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). OCAs shall ensure dissemination of new or revised SCGs to all derivative classifiers (including cleared contractors) as soon as practicable after the guide is approved.

5-3 RANKIN PROGRAM

1. The primary element of the RANKIN Program is a computerized database 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 S5513.7:	Mine Warfare Programs
OPNAVINST S5513.8:	Electronic Warfare Programs
OPNAVINST S5513.9:	Nuclear Warfare Programs
OPNAVINST S5513.10:	Advanced Technology and Miscellaneous Programs
OPNAVINST 5513.11:	Ground Combat Systems
OPNAVINST S5513.12:	Intelligence Research Projects
OPNAVINST 5513.13:	Non-Acoustic Anti-Submarine Warfare (NAASW) 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) web page 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 instructions are automatically distributed to commands consistent with their command missions. OCAs remain responsible for ensuring that new or revised guides are issued to those activities and contractors that handle their classified information pending re-issuance of the applicable 5513 instruction.

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) or the cognizant OCA.

5-4 PERIODIC REVIEW OF SCGs

Original Classification Authorities shall review their SCGs for accuracy and completeness at least every five 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

Security Classification Guides 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 A SCG

In cases of apparent conflict between a 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, as Amended, *Classified National Security Information*, 25 Mar 03

(b) OPNAVINST 5513.1F, *DON Security Classification Guides*, 7 Dec 05

CHAPTER 6

MARKING

6-1 BASIC POLICY

1. This chapter contains numerous examples of markings for classified material. These examples are all unclassified, and markings are used for illustration and training purposes only.

2. 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 6-1.6 for exceptions to this policy). "Associated markings" include those markings that 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).

3. Marking is required on all information technology (IT) systems and electronic media, including removable components that contain classified information (see paragraph 6-31, 6-32, and 6-34 for marking guidance). IT systems include any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. Electronic media includes Universal Serial Bus drives, flash drives, pen drives, compact disks, scanners, videotapes, floppy disks, recordings, etc. IT systems that process classified data, in forms other than traditional documents, such as weapon, navigation, and communication systems also require appropriate marking.

4. 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, emails, briefing slides (such as PowerPoint presentations), etc. Some types of classified material such as correspondence and letters of transmittal, recordings, photographs, file folders, and electronic messages, such as Naval messages, have special marking requirements as described in this chapter.

5. 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.

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

7. Exceptions to the basic marking policy include:

a. To preclude public acknowledgment, no classification level or associated markings shall be applied to any classified 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. Classified documents provided to foreign governments, their embassies, missions, or similar official offices within the U.S., shall be marked as described in paragraph 6-13.

d. Classified documents shall not be marked if the markings themselves would reveal a confidential source or relationship or a confidential human intelligence source 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. This marking 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 that cannot be marked in this manner. Also, see paragraph 6-34 for external markings on IT systems and electronic media.

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 6-3, 6-11 and 6-12, 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 also applies to emails on classified Information Technology (IT) systems (e.g., SIPRNET). Portion markings eliminate any doubt as to which portions of a document are classified, promoting more accurate derivative classification. 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" shall 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, photos 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, chart or photo. Mark chart, graph and photo 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 or 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 ODUSD (CI&S), 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 and 6A-4), when applicable. When subjects or titles of classified documents are included in the reference line, enclosure line, or the body of a document, the classification of the subject or title shall follow. This requirement does not apply to a reference or title that does not contain a subject; for example, “CNO (N09N2) ltr 5510 Ser 1234 of 5 Jun 05” would not require a portion marking. If the subject is included, it would require a portion marking to indicate the level of classification of the **title** of the document: “CNO (N09N2) ltr 5510 Ser 1234 of 5 Jun 05, “Vulnerabilities of the XYZ System (U)”.

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 6-25 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., COMSPAWARSYSCOM). 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. The list of sources shall identify the OCA(s) as well as the derivative sources.

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

1. Mark the face of a document containing only derivatively classified information with a "Derived from" line.

a. If all of the information was derivatively classified using a single Security Classification Guide (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).

b. If more than one SCG, source document, or combination of these, provide the derivative classification guidance, place "Multiple Sources" on the "Derived from" line. 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. Alternatively, if a limited number of sources is used, derivative classifiers are encouraged to list all of the sources on the “Derived from” line.

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 lowering of the classification level for the document will occur on a specific date or event. If a “Downgrade to” line is used, the “Declassify on” line must also be used (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.

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.

4. Declassification instructions and other downgrading instructions do not apply to documents containing Restricted Data (RD) or Formerly Restricted Data (FRD). Positive action by an authorized person is required to declassify RD or FRD documents. Only a Department of Energy (DOE) designated declassifier can declassify an RD document. Only a designated declassifier in DOE or an authorized DON OCA can make a declassification decision for an FRD document.

6-11 WARNING NOTICES AND ASSOCIATED MARKINGS

1. Warning notices advise document holders that additional protective measures such as restrictions on reproduction, dissemination or extraction are necessary.

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:

"REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR OR HIGHER DOD AUTHORITY."

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

b. **RD and FRD.** Per references (c) and (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. Note that 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):

"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 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)"). Place the short forms ("RESTRICTED DATA" or "FORMERLY RESTRICTED DATA") on interior pages, after the classification level at the top and bottom of each applicable page (e.g. "SECRET RESTRICTED DATA" or "SECRET FORMERLY RESTRICTED DATA"). 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 and marking requirements. 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, DOD DIRECTIVE 5210.2 APPLIES" 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 (d). Note that the RD warning notice is also required on the face of documents containing CNWDI.

d. **NNPI**

(1) Per reference (e), there is national policy prohibiting foreign disclosure of NNPI. There are special distribution control markings used on correspondence and documents containing classified or unclassified NNPI. Requirements for the proper use and placement of these markings are set forth in references (e) and (f) (these markings shall only be used on NNPI documents). Use of the NOFORN marking on NNPI is not to be confused with the NOFORN marking authorized for use as an intelligence control warning notice on classified intelligence information (see paragraph 6-12):

"NOFORN" - NOT RELEASABLE TO FOREIGN NATIONALS;

"SPECIAL HANDLING REQUIRED" - NOT RELEASABLE TO FOREIGN NATIONALS;
"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 associated markings on the face of a classified NNPI document (except an NNPI document also classified as RD) per reference (e).

(4) Classified NNPI containing RD or FRD information is governed by the provisions of paragraphs 6-5 and 6-10. Classified NNPI not containing RD or FRD information shall include the associated markings set forth in reference (e).

(5) Department of Energy Unclassified Controlled Nuclear Information (DOE UCNI). Mark unclassified NNPI which is also DOE UCNI per reference (e).

e. **SIOP**. Per reference (g), SIOP documents shall be marked in the same manner as any other classified document. SIOP documents released to NATO shall be marked per reference (g). NATO documents that contain details of the type and quantity described in reference (g) will include the following statement on the cover, the title page, and in the letter of promulgation:

"This document contains extremely sensitive information affecting the Single Integrated Operational Plan. Access to this document or the information contained herein shall be strictly limited commensurate with rigorously justified requirements. Use of military-controlled vehicles and two officially designated couriers is mandatory."

f. **SIOP-ESI**. Per reference (g), SIOP-ESI documents (e.g., correspondence, reports, studies, messages and any other media relaying SIOP-ESI) 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, followed by the above warning notice.

g. **COMSEC**

(1) Per reference (h), the designator "CRYPTO" identifies all COMSEC documents and keying material which are used to protect or authenticate classified or controlled 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 (CUI) are as follows:

a. **FOR OFFICIAL USE ONLY (FOUO) and FOR OFFICIAL USE ONLY (Law Enforcement Sensitive) (FOUO-LES)**

(1) **Documents containing FOUO.** Per references (i), mark the bottom front cover (if any), interior pages of documents, and on the outside back cover (if any) with "FOR OFFICIAL USE ONLY". Subjects, titles and each section part, paragraph, and similar portion of an FOUO document requiring protection shall be portion marked. Place the abbreviation “(FOUO)” immediately following the portion letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. 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."

(2) **Classified documents containing FOUO.** Per reference

(i), classified documents containing FOUO do not require any FOUO 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 unclassified portions containing only FOUO with "(FOUO)" immediately before the portion (see exhibit 6A-3). Classification markings take precedence over FOUO markings; mark portions that contain FOUO and classified information with the appropriate abbreviated classification designation (i.e., (TS), (S), etc.).

(3) **Documents containing FOUO-LES.** Per reference (i), mark documents containing FOUO Law Enforcement Sensitive (FOUO-LES) in the same manner as documents containing FOUO. Add "Law Enforcement Sensitive" to the FOUO marking, and "LES" to portion markings. Law Enforcement Sensitive information takes precedence over other FOUO information. Documents and portions containing both FOUO and FOUO-LES should be marked with the FOUO-LES markings.

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 Nuclear 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**. Per reference (i), 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**. Per reference (i), 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**. Per reference (i), 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 6-16.

f. **National Geospatial–Intelligence Agency (NGA) LIMITED DISTRIBUTION Information.** Mark information or material designated as LIMITED DISTRIBUTION, or derived from such information or material per reference (k), which contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat.

6-12 INTELLIGENCE CONTROL MARKINGS

1. The policy for marking intelligence information is contained in reference (l). 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 (l), or in other Director of Central Intelligence Directives.

(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").

(1) 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 intelligence 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").

(1) Use this marking to identify classified intelligence which, per reference (m), 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 TO") marking. The short form of this marking is "NOFORN"; the abbreviated form is "NF."

(2) Within the DON, only the Director of Naval Intelligence and the Director of Intelligence, United States Marine Corps, may determine what information warrants initial application of the "NOFORN" caveat. The "NOFORN" caveat shall not be applied to non-intelligence information except for NNPI (see paragraph 6-11). There is no other DON authorized use of the "NOFORN" marking on non-intelligence information. If documents marked with the "NOFORN" caveat are used for derivative classification, however, the derivative classifier should assume that the marking is correct until advised otherwise by the cognizant intelligence authority.

6-13 MARKING DOCUMENTS RELEASABLE TO FOREIGN NATIONALS

1. The "REL TO" control marking was previously only for use on intelligence information, but is now authorized for use on all classified defense information deemed releasable through appropriate foreign disclosure channels. Use the marking "RELEASEABLE TO USA//(applicable country trigraph(s), international organization or coalition force tetragraph)" ("REL" or "REL TO"), when information has been determined releasable through established foreign disclosure procedures to foreign nationals, international organizations or multinational forces. Further foreign dissemination of the material (in any form) is authorized only after obtaining permission from the originator.

2. The full marking "REL TO USA//(applicable country trigraph(s), international organization or coalition force tetragraph)" shall be used after the classification and will appear at the top and bottom of the front cover, title page, first page and the outside of the back cover, as applicable. "REL TO" must include country code "USA" as the first country code listed. Country trigraphic codes shall be listed in alphabetical order, after the USA, followed by international organization/coalition tetragraphic codes listed in alphabetical order. Country codes shall be separated by a comma and a space with the last country code separated by a space, and followed by two slashes (i.e., TOP SECRET//REL TO USA, EGY, ISR//) (See exhibit 6A-12).

3. The countries do not need to be listed when portion marking,

unless they are different from the countries listed in the “REL TO” designation at the top and bottom of the page. Text that is releasable to all the countries listed at the top and bottom of the page shall be portion marked “REL” (i.e., TS//REL). If the information is releasable to countries that are different than those listed in the overall “REL TO” marking, the portion marking has the same format, but with the specific countries and/or organizations listed alphabetically (See exhibit 6A-12). For example: Overall document marking is “SECRET//REL TO USA, NZL, NATO//.” Then the portion marking may be “S//REL TO USA, AUS, NZL, NATO,” to indicate that the information contained within this portion is also releasable to Australia.

4. Approved trigraphs (3 letter country code) are available at http://www.cia.gov/cia/publications/factbook/appendix/appendix-d.html and tetragraphs (4 letter country code) are available at http://www.odci.gov/cia/publications/factbook/appendix/appendix-b.html.

5. The “REL TO” marking is not authorized for use in conjunction with the marking "NOT RELEASABLE TO FOREIGN NATIONALS" ("NOFORN").

6. Existing documents originally marked “NOFORN” must be re-reviewed by the approved foreign disclosure authority (note that within the intelligence community, this is the originator of the intelligence) and when deemed releasable, remarked prior to release to foreign nationals. If the document is deemed releasable in its entirety, the “NOFORN” marking may be lined through and the document remarked with the revised overall page and portion markings. Any portions of a document not approved for release must be redacted. Remaining releasable portions of the document must be remarked as described herein. A record copy of the released document shall be annotated with the release authority (e.g., identity of the command with foreign disclosure authority, and source of release authority) making the release decision and the date of the decision. When circumstances warrant, notify all document holders of the release decision. The following are examples of an existing document originally marked “NOFORN.”

Overall, top and bottom of each page:

~~SECRET/NOT RELEASABLE TO FOREIGN NATIONALS~~
SECRET//REL TO USA, EGY, ISR//

Portion/paragraph: ~~(S/NF)~~ (S//REL)

Record copy: ~~SECRET/NOT RELEASEABLE TO FOREIGN NATIONALS~~
SECRET//REL TO USA, EGY, ISR//
(FOREIGN DISCLOSURE AUTHORIZED,
COMPACFLT, 8 FEB 05, DDL 05-03)

7. The intelligence control markings, "WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED" ("WNINTEL") and "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS" ("NOCONTRACT") are obsolete and 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 (l) for assistance in recognizing and identifying other obsolete intelligence control markings.

6-14 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 (n) 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)."

6-15 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, mark it as tentatively classified at the classification level deemed appropriate by the company, 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 canceled.

2. In any 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.

6-16 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 or international organization RESTRICTED information is included in an otherwise unclassified DON document:

a. NATO: 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 NATO RESTRICTED information" and mark the portions accordingly, i.e., “(NATO/R)."

b. Other Foreign Government Information: Mark the top and bottom of each applicable page with the following statement: “This page contains (Identity of foreign government) RESTRICTED information” and mark the portions accordingly, i.e., “(GBR/R).”

3. When NATO classified information is incorporated into a classified DON document, mark the document 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., "(NATO/S)" or "(NATO/C)").

4. A document containing FGI and marked with a classification designation which equates to RESTRICTED or an unclassified FGI document provided to a DON command on the condition that it be treated "in confidence," shall be marked "CONFIDENTIAL - MODIFIED HANDLING" with the identity of the originating government and whether the document is RESTRICTED or provided "in confidence" (see Chapter 7, paragraph 7-8, for safeguarding requirements).

5. When classified FGI is contained in a document:

a. Mark the face of the document with the following statement: "THIS DOCUMENT CONTAINS (indicate country trigraph(s) code or international organization tetragraph of origin) INFORMATION." If the identity of the foreign government or international organization must be concealed, "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION."

b. Mark portions to indicate the country trigraph code and classification level (e.g., "(GBR/C)" or "(DEU/S)"). No other markings are required on interior pages of DON documents containing FGI.

c. Mark the "Derived from" line with the identity of the U.S. and foreign sources. The "Declassify on" line shall contain a date or event for declassification as required by reference (o). Note, though, that no declassification action may be made on any document containing FGI unless and until permission has been obtained from the foreign government owning the information.

d. If the identity of the foreign government or international organization must be concealed, neither the derived from line nor the portion markings shall identify the foreign government. Instead, the abbreviated portion marking should indicate (“FGI/S”) and the derived from line shall be marked “Foreign Government Information,” along with the U.S. source of classification. A record copy identifying the source shall be maintained and properly protected.

6-17 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.

6-18 NICKNAMES, EXERCISE TERMS AND CODE WORDS

1. Reference (p) 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. Nicknames for Alternative Compensatory Control Measures (ACCM) (e.g., LIMIT FICTION) are assigned and approved via CNO (N09N2). The headers and footers of each applicable page of ACCM protected information shall identify the classification level and appropriate nickname (i.e., SECRET//LIMIT FICTION), in addition to the other markings required in chapter 6. These include warning notices, intelligence control markings and caveats, as appropriate. Similarly, each portion, part, paragraph and similar portion will, in addition to standard security classification markings, be marked with the ACCM nickname, e.g., (S/ACCM LIMIT FICTION). Only the full nickname may be used after the "ACCM" marking. No abbreviation of the nickname or any derivation of the nickname shall be used.

b. An exercise term is a combination of two non-code words that 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)").

6-19 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 rare, and in order to qualify for classification, something not already identified in the individual parts must be revealed. Classification by compilation must be based on an existing SCG or a new original classification decision by an approved OCA.

2. Place a statement on the face of a document classified by compilation which explains the reason(s) for classification or 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."

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.

6-20 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 that 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 and ink 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."

6-21 MARKING TRAINING OR TEST DOCUMENTS

1. Mark an unclassified training document, that 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) that will become classified when filled in.

6-22 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 computer printout portions, and briefing slides. 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.

6-23 REMARKING UPGRADED, DOWNGRADED OR DECLASSIFIED DOCUMENTS

1. Upon notification, holders of classified documents that have been upgraded, downgraded or declassified, shall immediately

re-mark the affected portions and, if applicable, overall classification markings on the cover page or first page of the document. Place on the face of the document the authority (OCA for the change, the name or personal identifier and position title of the person making the change(s) or declassification guide; and the date of the action); e.g., "PORTIONS DOWNGRADED TO CONFIDENTIAL PER NAVSEA LTR 5510 09T1 SER 5S345 OF 22 JUN 05 BY MS. J. SMITH ON 29 JUN 05," or "DECLASSIFIED PER OPNAVINST 5513.16B4 ON 18 NOV 04." Additionally, the overall classification markings on declassified documents shall be marked through with an "X" or lined through with a straight line.

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.).

3. An OCA with jurisdiction over the classified information may change the level of classification. Such changes shall be documented by remarking the new classification level, the date of the change, and the authority for the change. Affected portion markings shall also be remarked. Although changes may be promulgated by an OCA signed letter, the OCA must also immediately update affected security classification guides. The OCA must also immediately notify all holders of the information that the classification level has changed.

6-24 CLASSIFYING FROM SOURCE DOCUMENTS WITH OLD DECLASSIFICATION INSTRUCTIONS

1. A newly created document that derives its classification from a source document or SCG with an indefinite duration of classification from prior Executive Orders (e.g., OADR or X3), shall indicate that the source is marked with an indefinite duration of classification, and cite the date of the source. For example, a source document is marked X4, and the date of the source is 11 Nov 99. It would be marked as follows (see exhibits 6A-6 through 6A-8 for additional examples):

"Declassify on: Source marked X4, Date of Source: 11 Nov 99"

2. The "Date of Source" determines the duration of classification. As duration of classification is not normally authorized beyond 25 years, the new date for declassification would be 31 December 2024. When using source documents that have old declassification instructions, all declassification actions are effective on 31 December of the year in which declassification is to take place. Security classification guides, reference (o) and/or the OCA responsible for the

information should be consulted to ensure that no changes to the duration of classification have occurred.

6-25 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 (immediately beneath the official seal and before the first line of text) 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 (e)) (see paragraph 6-11) and all applicable intelligence control markings in their entirety (see paragraph 6-12).

2. **Letters of transmittal**. An unclassified letter of transmittal may have a classified document enclosed with or attached to it, but it is itself unclassified. A classified letter of transmittal may itself contain information classified equal to, or higher than, the classified document it is transmitting.

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), 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 and all applicable warning notices and intelligence control markings in the format prescribed in paragraphs 6-11 and 6-12. 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-13). Unclassified letters of transmittal shall not be portion marked. Interior pages of unclassified letters of transmittal, may be marked as "UNCLASSIFIED (top and bottom center)," but it is not required.

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) That 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 and all applicable warning notices and intelligence control markings in the format prescribed in paragraph 6-11 and 6-12. 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 that is SECRET, mark the transmittal, "SECRET—CONFIDENTIAL UPON REMOVAL OF ENCLOSURE (1)" (see exhibit 6A-14).

(2) That 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 and all applicable warning notices or intelligence control markings in the format prescribed in paragraph 6-11 and 6-12 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 itself is classified CONFIDENTIAL, but is transmitting a document classified SECRET/NOT RELEASABLE TO FOREIGN NATIONALS (enclosure (1)), mark the transmittal "SECRET/NOT RELEASABLE TO FOREIGN NATIONALS—CONFIDENTIAL 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.

6-26 MARKING ELECTRONICALLY-TRANSMITTED CLASSIFIED MESSAGES

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

a. Message processing systems should be designed such that the first item of the text shall be the highest overall classification level of the message, and when printed by an IT

system, the marking stands out from the rest of the text. 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, preformatted messages (such as RAINFORM, CASREP and similar reporting formats), which do not have identifiable portions, need not be portion marked. The overall classification, downgrading and declassification markings satisfy the marking requirements for these type messages.

d. The proper completion of the "Derived from" and "Declassify on" lines for messages is outlined in exhibit 6B.

2. When automated systems do not provide for automated marking of information, the individual creating the message is responsible for adding the appropriate markings when forwarding or storing messages.

6-27 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 cover sheets need not be attached when the file or folder is in secure storage.

6-28 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-15).

6-29 MARKING CLASSIFIED PHOTOGRAPHS, PHOTO SLIDES, 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-16).

2. Mark classified roll negatives and positives, and other film containing classified, with the 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.

6-30 MARKING CLASSIFIED BRIEFING SLIDES

1. Mark classified briefing slides, such as those produced using Microsoft PowerPoint or similar software, with the highest overall classification level and all applicable associated markings. If producing transparencies for projection, all markings required by this section must be used. In addition, any border, holder or frame shall be marked with the highest overall classification. Portion mark the information in the image area of the item (see **exhibit 6A-17**).

2. If a group of classified briefing slides is used together and maintained together as a set, mark only the first slide 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. Portion mark the information in the image area of the item (see exhibit 6A-17). Classified briefing slides permanently removed from such a set shall be marked as separate documents (see exhibit 6A-17).

6-31 MARKING CLASSIFIED MOTION PICTURE FILMS, VIDEOTAPES AND DIGITAL VIDEO DISCS (DVDs)

Mark classified motion picture films, videotapes and DVDs 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-18 and 6A-19).

6-32 MARKING CLASSIFIED SOUND RECORDINGS

All classified sound recordings shall have a clear audible statement announcing the highest overall classification level and all applicable associated markings 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-18 and 6A-19).

6-33 MARKING CLASSIFIED MICROFORMS

1. Mark classified microfilm, microfiche, and similar media with the highest overall classification level in the image area, so that it 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.

6-34 MARKING CLASSIFIED REMOVABLE IT STORAGE MEDIA AND IT SYSTEMS

1. Removable Storage Media Markings. Mark classified removable IT storage media with the highest overall classification level using the appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI IT 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 contained therein. Removable IT 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, magnetic diskettes, removable hard drives, thumb drives, tape cassettes, etc.). When the approved standard form labels are not feasible due to interference with operation of the system or because of the size of the media, other means for marking may be used so long as they appropriately convey the classification and other required markings (see exhibit 6A-20). In a totally unclassified working environment, there is no requirement to mark unclassified removable IT media.

2. IT System Marking.

a. External. Each IT system shall be marked to indicate the highest classification level of the information processed by the IT system and the network to which it is connected. This is especially important with systems that have the capability to switch from a classified network connection to an unclassified network or system. The appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI IT media)) shall be placed on IT systems and components with memory such as workstations, external hard drives, printers, copiers, portable electronic devices, servers, and back-up devices.

b. Internal. Program the software of classified IT systems storing or processing information in a readily accessible format, such as email processed on a classified IT systems, to mark each classified file stored or processed 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 per paragraphs 6-1 through 6-15, as applicable) (see exhibit 6A-21). When software does not provide for automated marking, information must nonetheless be marked. IT 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-20).

3. Where practicable, Information Assurance Managers shall ensure that IT systems provide for classification designation of data stored in internal memory or maintained on fixed storage media.

6-35 MARKING CLASSIFIED DOCUMENTS PRODUCED BY IT SYSTEMS

1. Mark documents produced on IT systems, to include emails generated on a classified IT system and those that function as word processing systems, per this chapter. Special provisions for marking some IT system 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 system 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 printouts removed for separate use or maintenance as individual documents (see exhibit 6A-22).

REFERENCES

(a) SECNAVINST 5720.42F, *DON Freedom of Information Act (FOIA) Program*, 6 Jan 99

(b) OPNAVINST 5513.1F, *DON Security Classification Guides*, 7 Dec 05

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

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

(e) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI)*, 26 Jul 05

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

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

(h) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

(i) DoD 5200.1-R, *DoD Information Security Program,* 14 Jan 97

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

(k) DoD Directive 5030.59, *National Imagery and Mapping Agency (NIMA) LIMITED DISTRIBUTION Imagery or Geospatial Information and Data,* 13 May 2003

(l) DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*, 11 Jul 01

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

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

(o) OPNAVINST 5513.16A, *Declassification of 25-Year Old DON Information*

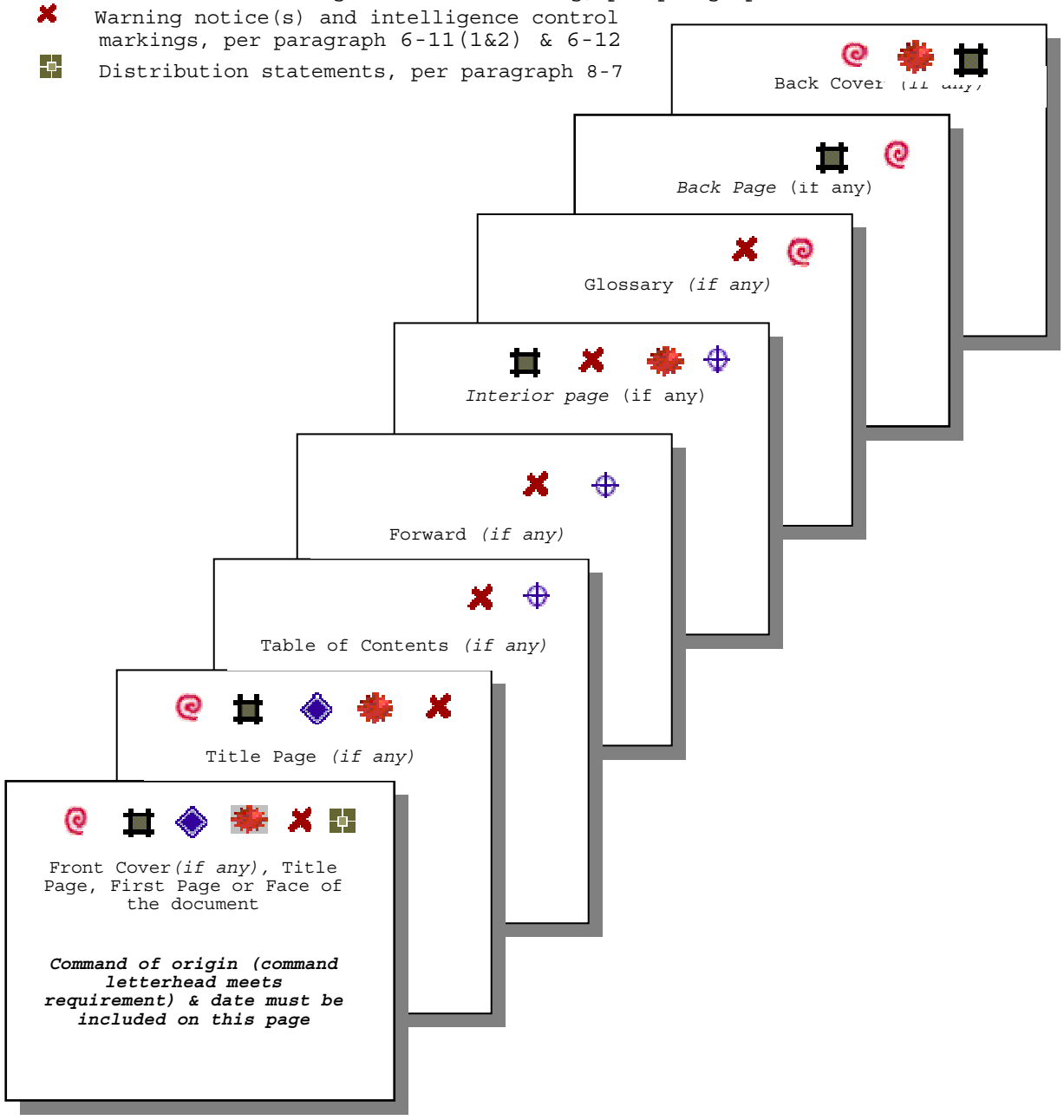
(p) OPNAVINST 5511.37C, *Policy and Procedures for the use of Nicknames, Exercise Terms and Code Words*, 22 Jul 97

EXHIBIT 6A

OVERALL AND PAGE CLASSIFICATION MARKINGS

(Refer to the paragraph noted in the ledger or exhibit 6A, for exact placement of markings)

Overall classification level (document), per paragraph 6-3
Interior page markings, per paragraph 6-4
Notices for Controlled Unclassified Information, per paragraph 6-11(3)
Associated markings, per paragraph 6-7 through 6-10
Releasable to foreign nationals marking, per paragraph 6-13(2)
Warning notice(s) and intelligence control markings, per paragraph 6-11(1&2) & 6-12
Distribution statements, per paragraph 8-7



CONFIDENTIAL

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

IN REPLY REFER TO

5510
Ser N09N2/9C123457
(Date)

CONFIDENTIAL

MEMORANDUM

From: N09N2
To: N1

Subj: PORTION MARKING AND OVERALL CLASSIFICATION (U)

Ref: (a) OPNAVINST S5513.3B, "Surface Warfare SCG (U)"
(b) Technical Report No. 1234, "Littoral Operations (C)"

1. (U) Apply portion markings to every part of a classified document (e.g. title, section, part, paragraph or subparagraph). The objective of portion marking is to eliminate doubt as to which portions of a classified document contain or reveal classified information. Titles or subjects of classified documents included in the reference line, enclosure line, or body of a letter shall be marked with the highest classification per paragraph 6-5.

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, and is marked "(U)" the abbreviation for "unclassified."

a. (C) This is subparagraph 2(a). If it were to contain "Confidential" information, this portion would be marked with the designation "C" in parenthesis.

(1) (C) This is subparagraph 2(a)1. If it were to contain "Confidential" information, this portion would also be marked with the designation "C" in parenthesis.

3. (C) The highest overall classification level of this document is "Confidential," based on its portion markings. Therefore, the document is marked "CONFIDENTIAL," top and bottom center, in slightly larger text.

J. DOE
Head, Information Security Policy

Derived from: Multiple Sources
Declassify on: Source marked X4, Date of Source: 7 Nov 2001

CONFIDENTIAL

THIS PAGE IS UNCLASSIFIED BUT MARKED "CONFIDENTIAL" 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 N09N2/7S123456
(Date)

SECRET

From: Chief of Naval Operations
To: Commandant, Naval District Washington

Subj: MARKING CLASSIFIED INFORMATION CONTAINING FOUO OR FOUO-LES INFORMATION (U)

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

a. (FOUO-LES) This is an example of portion marking a sub-paragraph containing "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" information. Indicate the appropriate abbreviated classification designation, i.e., (C), (S), (TS), for portions that contain both FOUO-LES and classified information. The same marking principle applies to portions that contain both FOUO and classified information. Indicate (FOUO-LES) for portions that contain both FOUO and FOUO-LES. Each portion of an "FOUO" or "FOUO-LES" document, to include subjects and titles, must be marked to ensure the information is protected.

2. (FOUO) FOUO and FOUO-LES information is by definition unclassified, thus "FOUO" or "FOUO-LES" is an acceptable portion marking substitute for "U." Additionally, pages that contain only FOUO or FOUO-LES information, with no classified information, may likewise be marked "FOR OFFICIAL USE ONLY" or "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" as an acceptable substitute for "Unclassified." When both FOUO and FOUO-LES are present in a document the overall marking will be "FOR OFFICIAL USE ONLY Law Enforcement Sensitive," as it takes precedence.

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

4. (FOUO) The marking "FOUO" or "FOUO-LES alerts holders that the information may be withheld under one or more of exemptions (b)(2) through (9) of the Freedom of Information Act (FOIA) Program, outlined in SECNAVINST 5720.42F. The marking "FOUO" or "FOUO-LES" 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. All known holders will be notified to remove this marking, if practical.

J. C. SMITH
Head, Information Security Branch

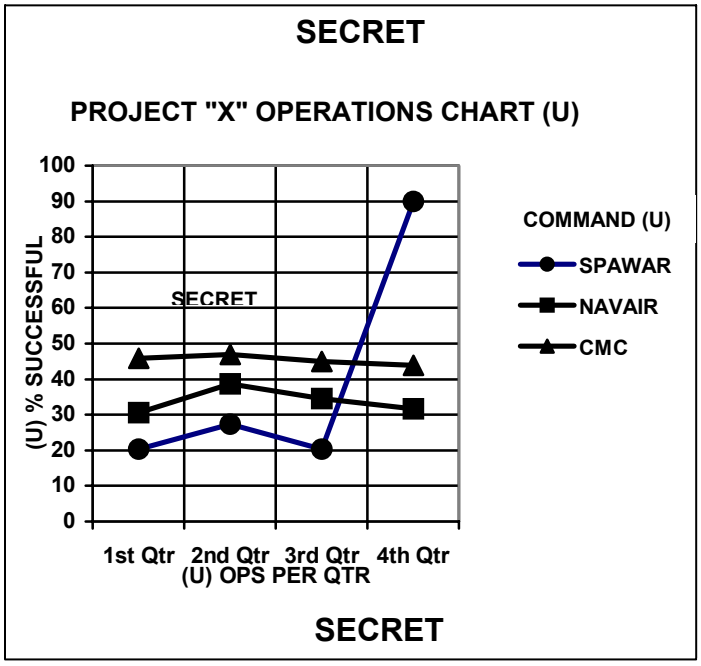
Derived from: OPNAVINST S5513.6C(4)
Declassify on: Source marked OADR, Date of source: 29 Dec 1989

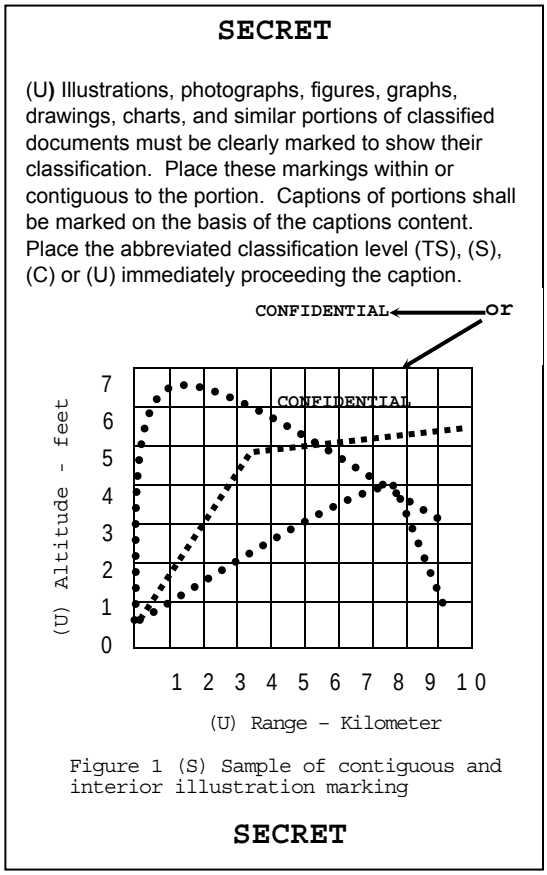
SECRET

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

SECRET

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 there abbreviated classification level in parentheses immediately following them. Blueprints, engineering drawings, maps and similar items shall be marked in the same manner.

SECRET

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

MEMORANDUM FOR THE COMMANDER NAVAL SEA SYSTEMS COMMAND

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

3. (U) FGI is subject to the 25-year automatic declassification provision of EO 12958, as Amended. However, no declassification action maybe taken without the approval of the foreign government that owns the information.

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

J. DOE
Special Assistant for Security

Derived from: Multiple Sources
Declassify on: 30 Sep 2020

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

"THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION" ***(for foreign government sources identified)***

SECRET

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

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

Subj: MARKING AN ORIGINALLY CLASSIFIED DOCUMENT (U)

Ref: (a) OPNAVINST 5513.1F

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, intelligence control markings, etc., per paragraph 6-11 through 6-13. A listing of "Reason" codes is found in reference (a).

3. (C) The OCA shall establish a date or event 25 years or less or specify the "25X1-Human" declassification instruction. The following are sample markings for originally classified documents:

a. (U) *Event as duration of classification:*
Classified by: PEO (Tactical Air)
Reason: 1.4(g)
Declassify on: Completion of XYZ Exercise

b. (U) *Date 25 years or less as the duration of classification:*
Classified by: COMNAVSEASYSCOM
Reason: 1.4(a)
Declassify on: 10 Oct 2010

c. (U) *"25X1" exemption:*
Classified by: Director, Naval Intelligence
Reason: 1.4(c)
Declassify on: 25X-1 Human

J. SMITH
Special Assistant for Naval Investigative
Matters & Security

Classified by: CNO(N09N)
Reason: 1.4(a)
Downgrade to: CONFIDENTIAL on 7 Jan 2008
Declassify on: 7 Jan 2010

SECRET

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 N09N2/6S123456
9 Jan 2006

SECRET

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

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

1. (S) Mark the face of the 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, intelligence control markings, etc. per paragraphs 6-11 through 6-13 of this policy manual.

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.

J. DOE
Program Manager

Classified by: Multiple Sources
Reason: 1.4a
Declassify on: 9 Jan 2031

SECRET

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

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

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, and all applicable warning notices, intelligence control markings, etc., per paragraphs 6-11 through 6-13. The duration of classification shall be specified on the "Declassify on" line. If deriving from multiple sources, cite the latest date or event that does not exceed 25 years. If deriving from a source(s) marked with an indefinite duration of classification from prior Executive Orders (e.g., OADR or X3), indicate the most restrictive duration of classification and cite the date of the source. The following are sample markings for derivatively classified documents:

a. (U) *Date or event 25 years or less as the duration of classification:*
Derived from: OPNAVINST S5513.3(11)
Declassify on: 12 Jan 2010

b. (U) *Source marked 25X1-Human:*
Derived from: ONI ltr 5500 Ser 00/S123 of 5 Jul 2004
Declassify on: 25X1-Human

c. (U) *Multiple sources: Source one prescribes declassification on 5 Sep 2006 and source two prescribes declassification on 21 Mar 2010.*
Derived from: Multiple Sources
Declassify on: 21 Mar 2010

d. (U) *Multiple sources: Source one prescribes declassification on 6 Jul 2020; Source two is dated 5 Aug 1985 and shows OADR on the "declassify on" line; Source three is dated 13 Apr 1997 and shows X3 on the "declassify on" line.*
Derived from: Multiple Sources
Declassify on: Source marked X3, Date of Source: 13 Apr 1997

2. (C) If one of the sources is more than 25 years old, and is exempt from declassification per OPNAVINST 5513.16, mark as follows:

a. (U) *Source contains classified information exempt from automatic declassification at 25 years and documented in OPNAVINST 5513.16:*
Derived from: OPNAVINST S5513.5B(38)
Declassify on: 25X4 and IAW OPNAVINST 5513.16

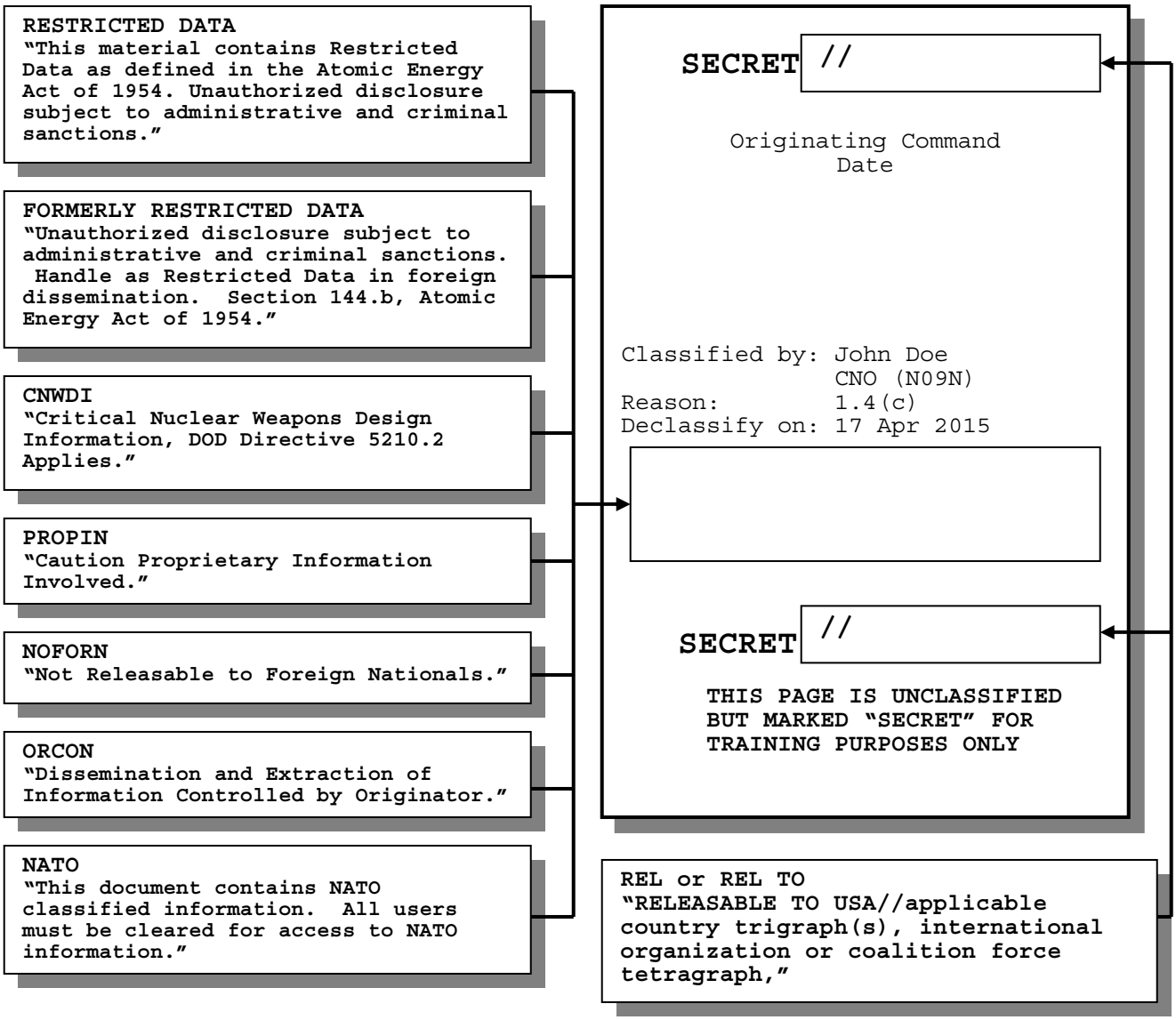
J. SMITH
Security Officer

Derived from: CNO ltr 5510 Ser 7U532200 of 22 Aug 05
Declassify on: 5 Sep 2010

SECRET

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

WARNING NOTICES, INTELLIGENCE CONTROL MARKINGS & INFORMATION RELEASABLE TO FOREIGN NATIONALS



Warning notices, intelligence control markings, and the releasable to foreign nationals caveat serve to notify holders that certain information requires additional protective measures (see paragraphs 6-11 through 6-13 or exhibit 6A for a complete listing and placement of these notices and markings).

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.

J. SMITH
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."

"CRITICIAL NUCLEAR WEAPONS DESIGN INFORMATION, DOD DIRECTIVE 5210.2 APPLIES."

SECRET

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

IN REPLY REFER TO
5510
Ser N09N2/9S123456
(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," "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 page.

2. (S/NF) Mark paragraphs and subparagraphs with the abbreviated form(s) of the appropriate intelligence control marking(s) (i.e., "NF," "PR" and "OC"). This abbreviated intelligence control marking follows the paragraph or subparagraph classification portion marking (separated with either a "/" or "-"). Mark tables, figures, and charts in a similar manner.

3. (U) 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.

J. DOE
By direction

Derived from: OPNAVINST 5513.4D-(17)
Declassify on: Source marked OADR, Date of Source: 15 Aug 87

SECRET/NOFORN/ORCON

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

SECRET//REL TO USA, EGY, ISR//

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//RELEASABLE TO USA, EGY, ISR//

From: Chief of Naval Operations (N09N2)
To: Commanding Officer, Space and Naval Warfare Systems Center Charleston

Subj: SAMPLE "REL TO" RELEASABLE TO FOREIGN NATIONALS CAVEAT (U)

1. (S//REL) The full marking "REL TO USA//applicable country trigraph(s), international organization or coalition force tetragraph" shall be used after the classification and will appear at the top and bottom of the front cover, title page, first page and outside of the back cover, as applicable.

a. (C//REL) "REL TO" must include country code "USA" as the first country code listed, with the country trigraphic codes and international/coalition tetragraphic codes listed in alphabetical order.

b. (S//REL) Information that is releasable to all the countries listed at the top and bottom of the page shall be portion marked "REL."

c. (C//REL) "REL TO" cannot be used with "NOFORN" on page markings. When a document contains both "NOFORN" and "REL TO" portions, "NOFORN" takes precedence for the markings at the top and bottom of the page.

2. (S//REL TO USA, AUS, EGY, ISR) Countries do not need to be listed unless they are different from the countries listed in the "REL TO" at the top and bottom of the page. This indicates that the information contained within this portion is also releasable to Australia.

J. SMITH
By direction

Derived from: OPNAVINST S5513.5B-(10)
Declassify on: 11 Oct 2015

SECRET//REL TO USA, EGY, ISR//

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET//RELEASABLE TO USA, EGY, ISR//" 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 N09N2/9U123456
(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, with the highest overall classification level and the applicable warning notices, intelligence control markings and the releasable to foreign nationals caveat, 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.

J. SMITH
By direction

SECRET

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--CONFIDENTIAL Upon removal of enclosure (2)

From: Chief of Naval Operations
To: Commander of Naval Installations

Subj: CLASSIFIED LETTER OF TRANSMITTAL (U)

Encl: (1) CNO ltr 5510 Ser N09N2/7U12345 of 10 Sep 04
(2) CNO ltr 5510 Ser N09N2/7SU56789 of 17 Feb 05

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 (i.e., enclosure (2)). The highest overall classification level is then Secret, but becomes 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.

a. (U) Portion mark the "enclosure" or "reference" line of a classified document, when the subject or title is included. For example, the overall classification level of the information contained in enclosure (2) is Secret, but the identifying information for enclosure (2) (i.e., *CNO ltr 5510 Ser N09N2/7U12345 of 10 Sep 04)* is not classified, as it does not reveal the subject or title of the document.

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 (i.e., enclosure (2)) is removed.

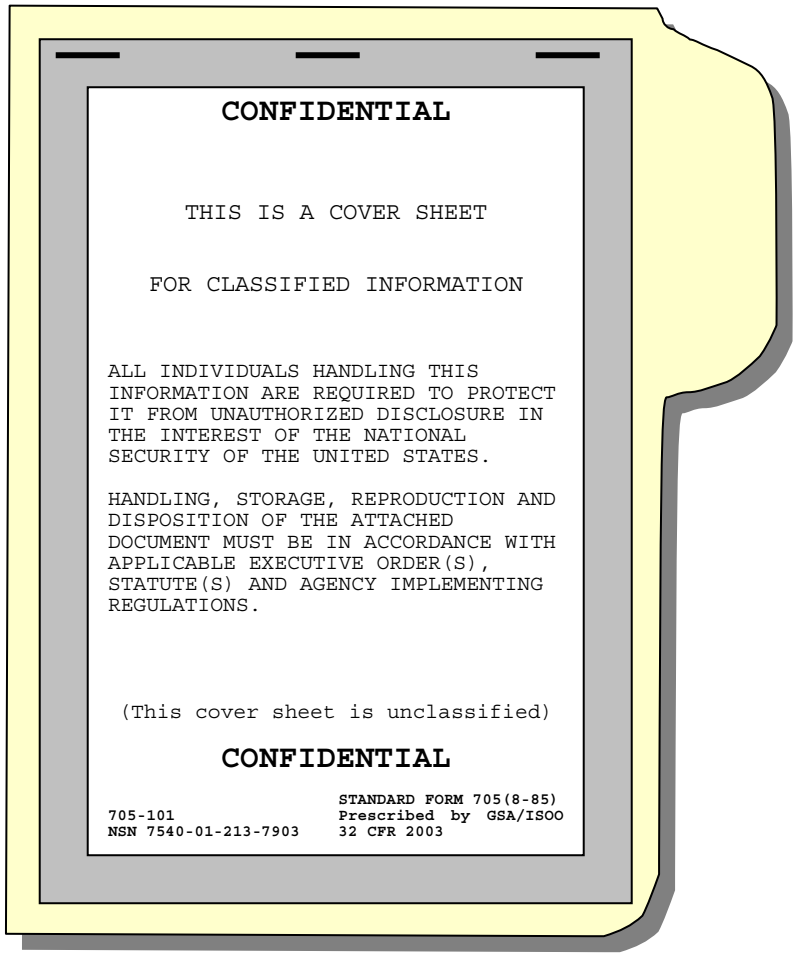
J. Smith
By direction

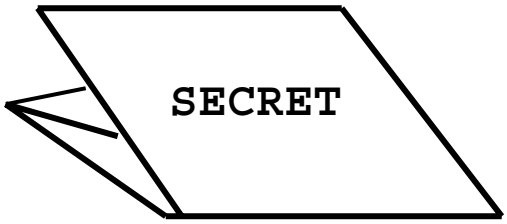
Derived from: Multiple Sources
Declassify on: 4 Dec 2009

SECRET

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

FILE FOLDERS, AND ROLLED OR FOLDED 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.

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

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

MARKING PHOTOGRAPHS

CONFIDENTIAL

(Back of Photograph)

Derived from: OPNAVINST S5513.3B (24)
Declassify on: 15 Jan 2016

23 July 2005

DEPARTMENT OF THE NAVY
Naval Sea Systems Command
Washington DC 20376-7007

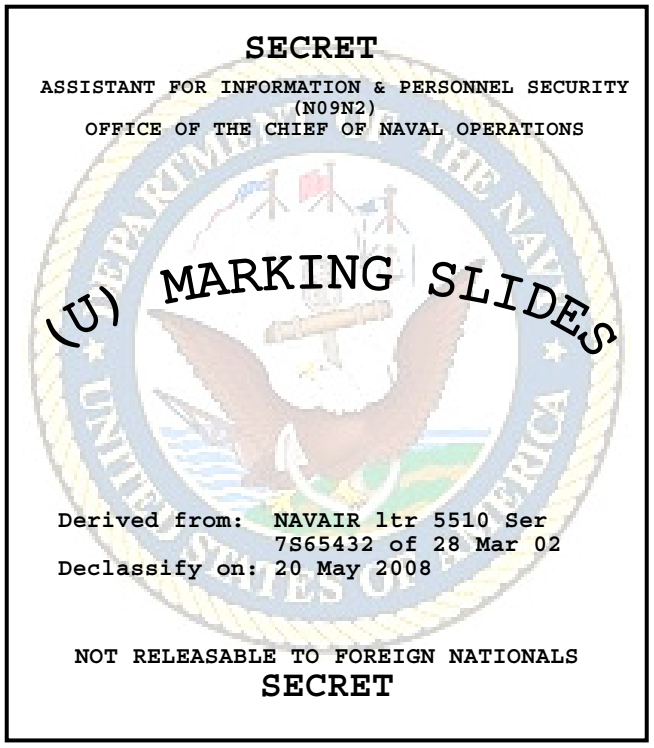
CONFIDENTIAL

PHOTOGRAPH

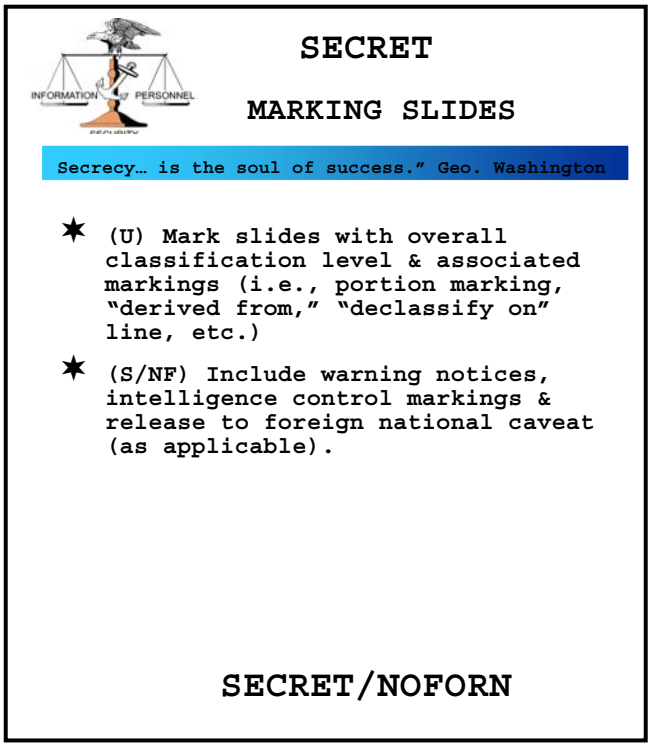
Mark the face of a classified photograph with its highest overall classification level and associated markings, if possible. If not, place these markings on the reverse side of the photograph. These markings may be stamped or permanently affixed by pressure tape, labels or other similar means. Marking requirements for photographs inserted or attached to documents generated on IT systems (i.e., email, MS PowerPoint, MS Word, etc.), apply as well.

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

MARKING SLIDES & TRANSPARENCIES



Cover Slide

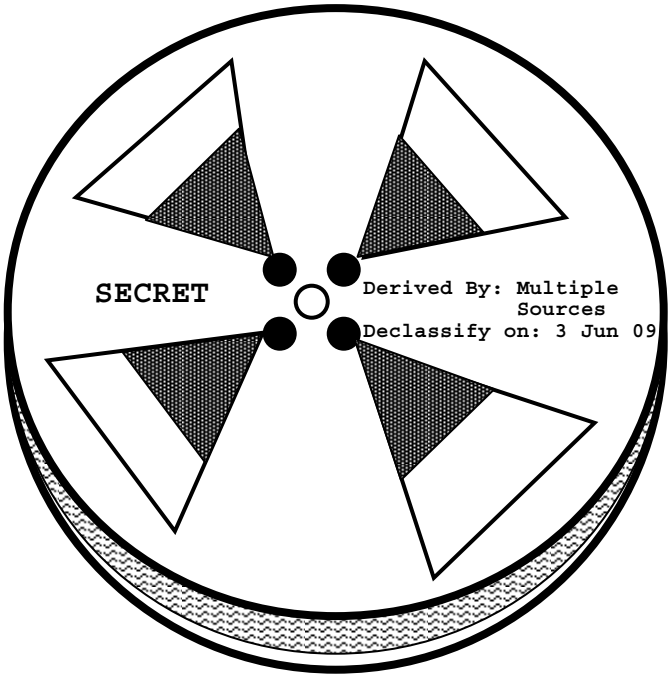


Interior Slide

Mark slides or transparencies, including those generated on IT systems (such as the example above using MS PowerPoint slides), 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/NOT RELEASABLE TO FOREIGN NATIONALS" FOR TRAINING PURPOSES ONLY

MOTION PICTURE FILM & CONTAINERS



FILM REEL

FILM CANISTER

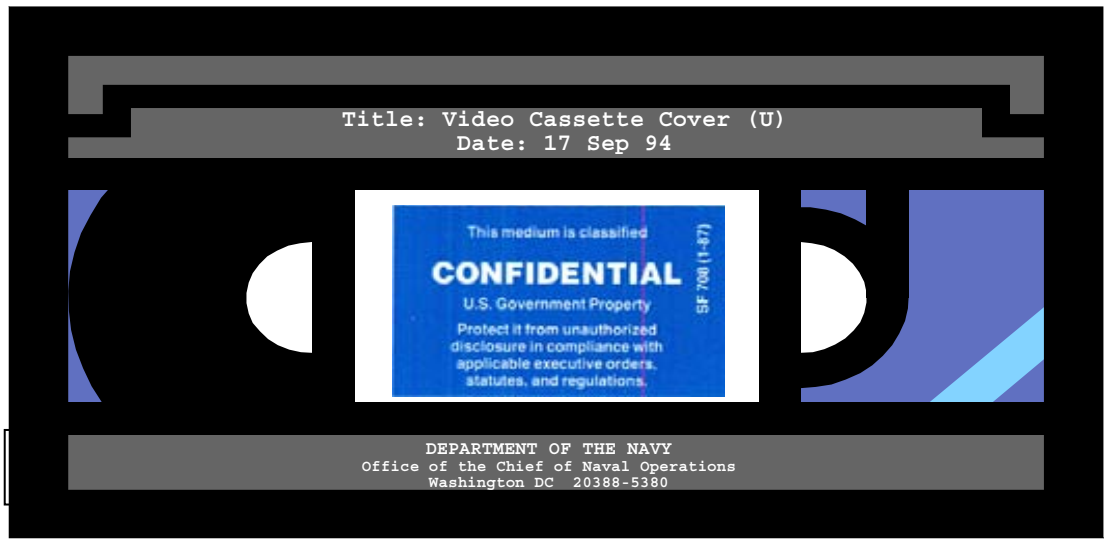
Classified motion picture films, videotapes and their titles shall be prominently marked, visible when projected, at the beginning and end of the production with the highest overall classification level and associated markings of the information they contain. Mark classified films, videotapes, and their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

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.

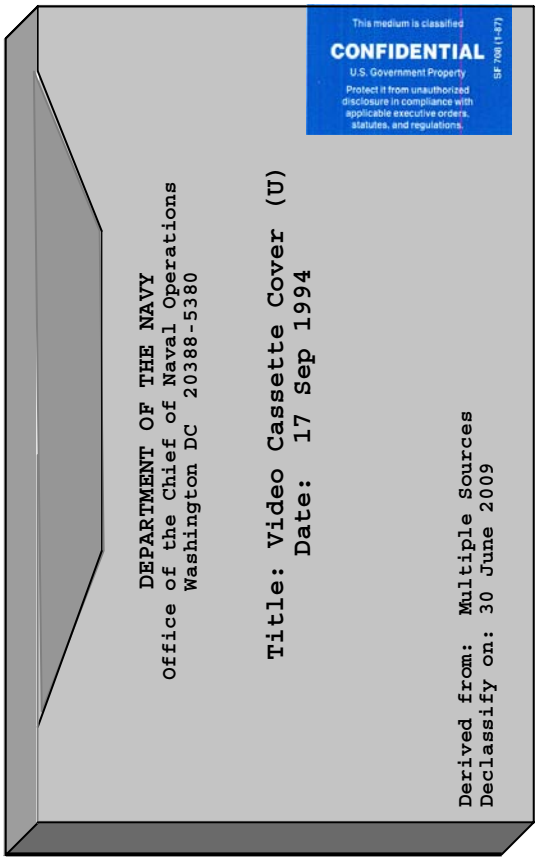
THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

VIDEOTAPES AND DVDs

The marking requirements of exhibit 6B-18 also apply to this exhibit.



VIDEOTAPE

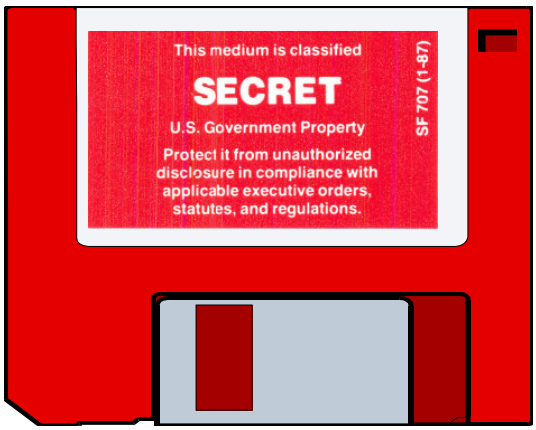


VIDEOTAPE CONTAINER

DIGITAL VIDEO DISC (DVD)

REMOVABLE IT MEDIA

Removable storage media and devices used with IT systems and word processors shall be marked using the appropriate SF label to indicate the highest overall classification level of information contained therein. Samples indicated below with recommended means for marking.



Disk: Use applicable SF label, i.e., SF-706, 707, 708, 710 or 712 (see below)

CD: Write on or affix a CD label

USB flash or thumb drives: Order with classification level printed; or affix colored tape that matches the color schematic of the SF labels & write the classification level

Standard Form IT labels:
Top Secret: SF-706
Secret: SF-707
Confidential: SF-708
Unclassified: SF-710

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

MARKING EMAIL ON CLASSIFIED IT NETWORK

To: John Smith
Cc: J. Jones
Subj: SAMPLE OF A CLASSIFIED EMAIL ON SIPRNET (U)

SECRET

John Smith,

1. (U) This is a sample of a classified email sent via a classified network, such as SIPRNET.

a. (C) The marking requirements (i.e., overall, portion and associated markings) still apply when creating an email on a classified network like SIPRNET, to include attachments.

2. (S) An email created on SIPRNET is considered a final document and not a working document, and must be marked as such.

3. (U) If you have any questions, I can be reached at (555) 555-5555.

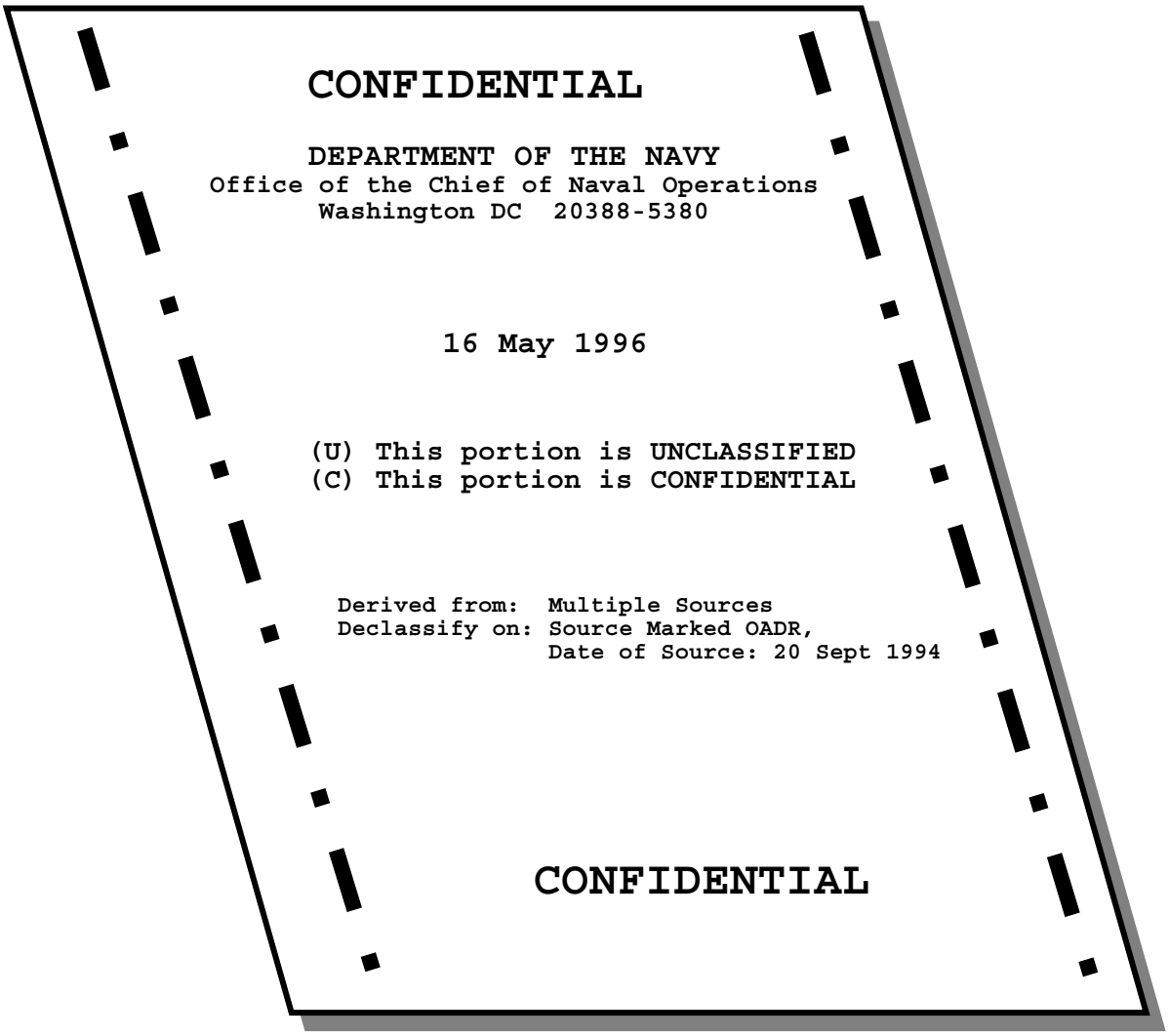
r/Jane Doe
Information Security Specialist
CNO (N09N2)

Derived from: OPNAVINST S5513.6C(4)
Declassify on: Source marked X5, Date of Source: 29 Dec 2002

SECRET

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

PAGES OR PORTIONS REMOVED FROM IT PRINTOUTS



Mark pages or portions removed from IT 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. The interpretation of Executive Order (EO) 12958, as Amended is that messages shall be marked in a manner similar to documents. The highly formatted and abbreviated nature of military messages introduces some eccentricities into the marking of classified messages. However, classified messages shall indicate (1) the highest classification level of the information contained in the document, (2) the nature of the classification (i.e., original or derivative), (3) the source of classification, (4) the reason for classification (if applicable), (5) downgrading instructions (if applicable), and (6) declassification instructions

2. The Navy is transitioning to a software application called Common Message Processor (CMP). CMP facilitates message drafting and aligns the Navy with the rest of the Joint community by standardizing message preparation software. The current DON approved version of CMP is 4.6.05 patch five (P5).

3. CMP has a drop down menu, in the header of the message, to select the highest overall classification level of the information contained in the message. Whereas in the body of the message, there is a "DECL" set that will guide users to fill in the appropriate fields. However, Fields 2 and 4 in the "DECL" set are pending modification, in order to reflect the classification marking changes in EO 12958, as Amended. The recommended implementation date for changes to Field 2 is March 2006, and March 2007 for Field 4. The guidance and examples outlined in this exhibit should provide ample instruction on the correct use of the "DECL" set, to include some interim workarounds until Fields 2 and 4 are modified.

"DECL"

Field 1: "Derivative or Original Source for Classification" Abbreviated as field descriptors, **"DERI:"** or **"ORIG:"**. This is a mandatory field. Keep in mind that the majority of DON classified messages will be derivative classification decisions, as DON original classification decisions are a rare occurrence.

Field 2: "Reason for Classification" Do not use this field at this time. It has not been modified to reflect the changes to the reason codes (i.e., 1.4A through 1.4H vice 1.5A through 1.5G) in EO 12958, as Amended. Typically, this field is mandatory if the field descriptor cites **"ORIG,"** as it reflects the rare

occurrence of an original classification decision. In the interim, OCA's shall enter the applicable reason code, indicated in Table 1, in the string of text in Field 3.

TABLE 1

(The "Reason Codes" parallel the eight EO 12958, as Amended classification categories, e.g., 14A is equivalent to classification category 1.4(a) of EO 12958, as Amended)

REASON	
14A	Military plans, weapons systems, or operations
14B	Foreign government information
14C	Intelligence activities (including special activities), intelligence sources or methods, or cryptology
14D	Foreign relations or foreign activities of the United States, including confidential sources
14E	Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
14F	United States Government programs for safeguarding nuclear materials or facilities
14G	Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
14H	Weapons of mass destruction

Field 3: "Downgrading or Declassification Instructions" This field is mandatory, until Fields 2 and 4 are modified to reflect the changes to EO 12958, as Amended. Once the modifications have been implemented, this field will be "conditional," depending on whether the applicable declassification instruction is entered in Field 3 or 4. In the interim, the following guidance provides workarounds for entering data that is normally applied in Fields 2 and 4, along with standard entries for this field. Field 3 has two field descriptors. One is abbreviated as **"INST:"** when indicating downgrading instructions on original or derivative classification decisions, to indicate the reason code for original classification decisions, when communicating declassification guidance upon completion of an exercise or event, or when the source document is marked with an indefinite duration of classification from prior Executive Orders (i.e., OADR or "X" codes). The other is abbreviated as **"DATE:"** when indicating an actual declassification date.

Field 4: "Downgrading or Declassification Exemption Code" Do not use this field at this time. It has not been modified to reflect the changes (i.e., elimination of "X" codes) in EO 12958, as Amended. Typically, this field is "conditional,"

depending on whether Field 3 is completed. In the interim, enter the applicable automatic declassification exemption category, indicated in Table 2, in the string of text in Field 3, when applicable.

TABLE 2

(Below are the 25-year automatic declassification exemption categories. Original Classification Authorities (OCA's) may use "25X1" for Human Intelligence if they have the authority to originally classify such information. Derivative classifiers may only specify an approved "25X" exemption category if the information is derived from a source document that is over 25 years old, is so marked, and the information is contained in the DON ISCAP approved declassification guide (OPNAVINST 5513.16B).

Category	
25X1	Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method
25X2	Reveal information that would assist in the development or use of weapons of mass destruction
25X3	Reveal information that would impair U.S. cryptologic systems of activities
25X4	Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon systems
25X5	Reveal actual U.S. military war plans that remain in effect
25X6	Reveal information, including foreign government information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States
25X7	Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized
25X8	Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security
25X9	Violate a statute, treaty, or international agreement

IMPORTANT NOTE: Typically, Fields 2, 3 and 4 form a repeatable group of fields per USMTF rules.

4. The following are examples of completed "DECL" sets for classified USMTF messages:

EXAMPLE 1: DECL/DERI:MULTIPLE SOURCES/-
/INST:SOURCE MARKED X4,DATED 01JUN1986//

EXAMPLE 2: DECL/DERI:OPNAVINST 5513.4D(17)/-
/INST:SOURCE MARKED OADR,DATED 15AUG1987//

EXAMPLE 3: DECL/DERI:ONI LTR 5500 SER 00-S123 OF 5JUL2004/-
/INST:25X1-HUMAN//

EXAMPLE 4: DECL/DERI:OPNAVINST S5513.5B-38/-
/INST:25X4,OPNAVINST 5513.16B//

EXAMPLE 5: DECL/DERI:PEO TACTICAL AIR LTR/-
/INST:COMPLETION OF XYZ EXERCISE//

NOTE: In examples 1 through 5, only the mandatory field (Field 1) and the conditional field (Field 3) have data to be reported. A "No data sign" (-) hyphen is automatically inserted by CMP in Field 2, if Fields 3 or 4 are completed, to maintain set integrity. Examples 1 and 2 show the application of a source document(s) marked with an indefinite duration of classification from prior Executive Orders (i.e., "X" codes or OADR). Keep in mind, if you have multiple sources each marked with varying "X" codes or OADR (i.e., *Source 1 is dated 5 Aug 89 and shows OADR on the declassify on line; Source 2 is dated 13 Apr 98 and shows X3 on the declassify on line; and Source 3 is dated 3 Jul 01 and shows X5 on the declassify on line*), indicate the declassification date of the document with the latest date for the field descriptor **"INST:"** (i.e.: INST:SOURCE MARKED X5,DATED 3JUL2001). Examples 3 and 4 show the application of the "25X" automatic declassification exemption categories for derivative classification decisions, until Field 4 is modified to reflect the changes to EO 12958, as Amended. Example 5 shows the application of a declassification date based on an event or exercise.

EXAMPLE 6: DECL/DERI:USS RUSHMORE 252359ZJAN2001/-
/INST:DOWNGRADE TO (C) ON 01FEB06/-/-/DATE:20MAY2008//

NOTE: In example 6, a "No data sign" (-) hyphen is automatically inserted by CMP for Field 2, if Fields 3 or 4 are completed. This maintains set integrity. A "No data sign" (-) hyphen is also automatically inserted by CMP for Field 4, when Fields 2, 3 or 4 are repeated as a group of fields. Again, this maintains set integrity. An alternate content must be used for Field 3, so that the field descriptor "DATE:" can be used.

EXAMPLE 7: DECL/DERI:CG-W-5/-/INST:DO NOT DECLASSIFY//

NOTE: In example 7, the classified message contains RD. Documents, to include messages, containing RD and FRD do not bear declassification instructions. Enter into Field 3 "INST:DO NOT DECLASSIFY//" A "No data sign" (-) hyphen is automatically inserted by CMP for Field 2, if Fields 3 or 4 are completed. This maintains set integrity.

EXAMPLE 8: DECL/ORIG:ONI/-/INST:REASON 14A/-/-/INST:25X1-HUMAN//

EXAMPLE 9: DECL/ORIG:COMNAVSEASYSCOM/-/INST:REASON 14A/-/-/DATE:1OCT2010//

NOTE: In examples 8 through 9, the reason code is entered in Field 3, until Field 2 is modified to reflect the changes to EO 12958, as Amended. A "No data sign" (-) hyphen is automatically inserted by CMP for Field 2, if either Fields 3 or 4 are completed. This maintains set integrity. These examples also show various applications of the declassification date.

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 State SECRET DRZAVA TAJNA	TAJNO Military SECRET VOJNA TAJNA	POVERLJIVO	
Belgium(French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTS
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	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) NEPOZVOLEN (Illicit) 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
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN			
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL	DIFFUSION RESTREINTE

Country	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	
Greece	AKP/ AOPPHTON	AOPPHTON	EMITEYTIKON	EPIPIMENH XPHE
Guatemala	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				
Korea	KUP PI MIL	KUP PI MIL	KUP PI MIL	
Kyrgyzstan 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

Country	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
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
Romanian	ULTRASECRET	SECRET	CONFIDENTIAL OR SECRET	RESTRINS
Russian	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	HEMLIG		
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				
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Turkey	COK GIZLI	GIZLI	OZEL	HIZMET OZEL
Turkmenistan 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				
Viet Nam(French)	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
(Vietnamese)	TOI-MAT	MAT	KIN	TU MAT

CHAPTER 7

SAFEGUARDING

7-1 BASIC POLICY

1. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited Information Technology (IT) systems, 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. In addition to safeguarding classified information, commanding officers shall ensure that controlled unclassified information (CUI) is safeguarded from unauthorized access by the public. Measures shall be taken to protect IT systems which store, process, and transmit such information from unauthorized access.

3. 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.

4. Foreign national access to CUI shall be in accordance with reference (b).

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 register or log. The register or log shall completely identify the information, and at a minimum include the date originated or received, individual serial numbers, copy number, title, originator, initial page count, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken. If a disposition action such as destruction, downgrade or declassification affects the initial document page count, the page count does not need to be changed in the register or log if a list of the effective pages (LOEPs) is contained within the document. Per reference (c), Top Secret registers or logs shall be retained for five years.

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. Top Secret Control Officers (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 policy manual. See chapter 9, paragraph 9-10, for receipting requirements for Secret classified information.

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 policy manual.

7-6 SECRET AND CONFIDENTIAL WORKING PAPERS

1. Secret and Confidential working papers such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain Secret or Confidential information shall be:

a. Dated when created;

b. Conspicuously marked centered top and bottom of each page with the highest overall classification level of any information they contain along with the words "**Working Paper**" on the top left of the first page in letters larger than the text;

c. Protected per the assigned classification level; and

d. Destroyed, by authorized means, when no longer needed.

2. Commanding officers shall establish procedures to control and mark all Secret and Confidential working papers in the manner prescribed for a finished document when retained more than 180 days from the date of creation or officially released outside the organization by the originator. A document transmitted over a classified IT system is considered a finished document.

7-7 TOP SECRET WORKING PAPERS

The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain Top Secret information.

7-8 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. Control and safeguard special types of classified information as follows:

a. **NWPs**. Reference (d) 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 (e).

c. **FGI**. Control and safeguard FGI, other than NATO, in the same manner as prescribed by this policy manual 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 five years per reference (c).

(3) SECRET FGI. Maintain records for the receipt, internal distribution, transmission and destruction of Secret FGI. Secret FGI may be reproduced to meet mission requirements and reproduction shall be recorded. Retain records for three years per reference (c).

(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 two years per reference (c).

(5) FOREIGN GOVERNMENT RESTRICTED and UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE. The degree of protection provided to this type of 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 (f).

e. **SCI**. Control and safeguard SCI per reference (g).

f. **COMSEC**. Control and safeguard COMSEC information per reference (h).

g. **SIOP and SIOP-ESI**. Control and safeguard SIOP and SIOP-ESI per reference (i).

h. **SAPs**. Control and safeguard SAP information per reference (j).

i. **NNPI**. Control and safeguard NNPI per reference (k).

j. **FOUO**. Control and safeguard FOUO information per reference (l).

k. **SBU INFORMATION**. Control and safeguard SBU information in the same manner as FOUO, per reference (l).

l. **DEA SENSITIVE INFORMATION**. Control and safeguard DEA Sensitive information in the same manner as FOUO, per reference (l).

m. **DoD UCNI**. Control and safeguard DoD UCNI per reference (m).

7-9 ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM)

1. When an Original Classification Authority (OCA) determines that other security measures detailed in this policy manual are insufficient for establishing "need-to-know" for classified information, and where Special Access Program (SAP) controls are not warranted, Alternative Compensatory Control Measures (ACCM) may be employed. The purpose of ACCM is to strictly enforce the "need-to-know" principle. Additional security investigative or adjudicative requirements are not authorized for establishing access requirements for ACCM information.

2. The following ACCM controls are authorized:

a. An unclassified nickname assigned in accordance with reference (n) and coordinated through CNO (N09N2).

b. A list of persons granted access to the ACCM protected information.

c. Placing classified ACCM information in sealed envelopes marked only with “ACCM,” the classification level, and nickname and stored in a manner to avoid commingling with other classified information.

d. Special markings to identify information as being controlled by ACCM.

e. A system that provides for recurrent oversight and inspection of ACCM by representatives of the cognizant OCA or CNO (N09N2).

3. ACCM Limitations:

a. ACCM shall not use codewords as defined in reference (n), nor shall they use the assigned nickname if it is not preceded by the acronym "ACCM."

b. ACCM shall not be used for NATO or non-intelligence Foreign Government Information (FGI) without the prior written

approval of the ODUSD (Policy). Any such request must be submitted via CNO (N09N2).

c. ACCM shall not be used to protect classified information in acquisition programs as defined in reference (o), nor shall ACCM be used during the acquisition process to protect technical or operational item characteristics, funding, capabilities or vulnerabilities. However, systems that are in operational use do not fall under the acquisition process definition. Likewise, improvements to operational systems are not considered in the acquisition process. These are considered fielded end items, and are eligible for ACCM status if properly justified.

d. ACCM shall not be used to control classified information designated as Restricted Data (RD), Formerly Restricted Data (FRD), Communications Security (COMSEC) or Sensitive Compartmented Information (SCI).

e. ACCM shall not be used for unclassified information.

f. An ACCM specific Non-Disclosure Agreement shall not be used.

g. ACCM shall not use a billet structure or system to control the position and numbers of persons with access to ACCM.

h. The use of ACCM measures shall not preclude, nor unnecessarily impede, Congressional, Office of the Secretary of Defense, or other appropriate oversight of programs, command functions, or operations.

4. The CNO (N09N2) approves the use of ACCM, and ensures that the protection afforded classified information is sufficient to reasonably deter and detect loss or compromise. Each request for the establishment of ACCM shall consider the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and countermeasures benefits versus cost when assessing the need to establish an ACCM.

a. Requests must be submitted, in writing, by the cognizant OCA. The request must include a justification for application of ACCM and a security plan. The security plan shall describe how control measures will be implemented; identify the CNO (N09N2) approved nickname and describe how information will be marked with the nickname; provide a description of the

information requiring additional control measures; and describe roles and responsibilities for implementation and oversight of the ACCM.

b. The CNO (N09N2) shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for their use, and shall report annually to the ODUSD (Policy). OCAs with approved ACCM shall provide program information as requested by CNO (N09N2) for inclusion in the report.

6. Safeguarding. Standard Form classified material cover sheets may be used, but must be stamped or marked with the ACCM markings. The Director of Security, ODUSD (CI&S), via CNO (N09N2), may authorize the use of specially designed cover sheets.

7. Transmission. ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

a. ACCM information wrapped for transmission shall have the inner envelope marked with the ACCM nickname and must be addressed to the attention of an individual authorized access to the ACCM information.

b. The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending over secure facsimile.

8. Electronic files containing ACCM protected information shall be configured and designated to ensure that access is restricted to individuals with authorized access. Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing classified information at the same level may be used to transmit ACCM information. Each such transmission must be marked as described above and in Chapter 6, and transmitted only to those authorized access to the ACCM information.

9. Personnel requiring access to ACCM protected information shall receive specialized training regarding the procedures for access, control, transmission, storage, marking, etc. Individuals may be required to sign an acknowledgement of

training should the security plan so specify.

10. Contractors. Approved ACCM may be applied to cleared DoD contractors only when identified in the Contract Security Classification Specification, DD Form 254.

11. Activities and individuals having responsibility for protecting ACCM information (including contractors) shall be provided a copy of the ACCM security plan, as appropriate.

12. Security Classification Guide. The requirement for ACCM shall be included in security classification guides for the protected information. An ACCM-specific security classification guide is not necessary.

13. ACCM shall be cancelled as soon as they are no longer necessary. Requests for cancellation must be submitted to CNO (N09N2), in writing. CNO (N09N2) will notify ODUSD (Policy).

7-10 CARE DURING WORKING HOURS

1. Keep classified information under constant surveillance by an authorized person and covered with classified material cover sheets (SFs 703, 704, or 705) when removed from secure storage.

2. Protect preliminary drafts, plates, stencils, 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.

3. Classified discussions shall not be conducted in public conveyances or places that permit interception by unauthorized persons, and classified material may not be opened or read in any area where it can be seen by unauthorized individuals.

7-11 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 security containers have been properly secured at the end of the day. The SF 701 and 702 shall also be annotated to reflect after

hours, weekend and holiday activities. These forms may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation required by Chapter 12.

7-12 SAFEGUARDING DURING VISITS

Commanding officers shall establish procedures to ensure that only visitors with an appropriate eligibility determination and need-to-know are granted access to classified information. At a minimum, these procedures shall include verification of the identity, eligibility level, access (if appropriate), and need-to-know for all visitors. Refer to reference (p) for visit procedures.

7-13 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 may only be held 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 shall assume security responsibility for the meeting. Security precautions must be taken for conference rooms and areas specifically designated for classified discussions. Technical surveillance counter-measures support for meetings involving Top Secret information, and for other designated classified discussion areas (e.g., base theaters, school auditoriums, unsecured classrooms, etc.) must be requested per reference (q).

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 and/or cleared DoD contractor employees. Any participation by foreign nationals or foreign representatives shall be approved, in writing, by the DON command foreign disclosure officer or the Navy International Programs Office

prior to attendance to ensure that the information to be presented has been cleared for foreign disclosure. All attendees shall have an appropriate clearance eligibility 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. Identification of the U.S. Government employee nominated to function as the security manager;

f. The specific reason for having the meeting;

g. A security plan specifying procedures for verifying access eligibility, badging procedures, access control procedures, and procedures for storing the classified information;

h. A draft agenda, announcement, and eligibility verification form; and

i. 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. The individual designated as security manager by the sponsor shall be responsible for providing and maintaining physical security for the actual site of the classified meeting. Other U.S. Government organizations or cleared contractor facilities 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.

6. Classified meetings may not be held at hotels, conference centers or any other uncleared venue.

7-14 SAFEGUARDING U.S. CLASSIFIED INFORMATION IN FOREIGN COUNTRIES

1. U.S. classified information transported to foreign countries must be safeguarded as described below (see exhibit 2B for emergency destruction plans).

a. At a U.S. military installation, or a location where the U.S. enjoys extraterritorial status, such as an embassy or consulate;

b. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel;

c. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host government control, provided the classified information is stored in GSA-approved security containers and is placed under 24-hour control by U.S. Government personnel; or

d. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control provided the classified information is secured in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access.

3. To the extent possible, and without adversely affecting operational efficiency, U.S. classified information that has been determined by appropriate authority to be releasable to the host government will be segregated from information which has not been authorized for release. If the volume of classified information makes it impractical to store releasable classified information in one security container and non-releasable classified information in another, than the classified information may be stored in different drawers of the same security container. When segregation is not feaseable or practical, a waiver may be requested from CNO (N09N2).

4. Foreign personnel shall be escorted in areas where U.S. non-releasable classified information is handled or stored. As an alternative in the case of exchange officers, and when required by operational necessity, unescorted access by foreign personnel may be allowed during duty hours to areas where U.S. non-releasable classified information is stored in a locked security container or is under the direct, personal supervision of U.S. personnel.

7-15 REPRODUCTION

1. Classified 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. Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for

classified reproduction (see paragraph 7-8.1.c. for reproduction of FGI).

2. Commanding officers shall:

a. Designate specific equipment for classified reproduction;

b. Ensure that all copies are subject to the same controls as the original information;

c. Limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk;

d. Comply with reproduction limitations placed on classified information by originators and special controls applicable to special types of classified information; and

e. Facilitate oversight and control of reproduction.

3. When selecting reproduction equipment, ensure that the equipment does not have an internal hard drive or non-volatile memory. If it does, you must protect the equipment at the highest level of classified material reproduced.

a. If the reproduction equipment is networked to other IT systems or equipment, the whole network must be provided security protection and approved to process classified material at the highest level of classified material reproduced.

b. Before permitting uncleared maintenance personnel access to or releasing reproduction equipment that has been used for processing classified material, inspect the equipment to ensure that no classified material has been left in the equipment.

REFERENCES

(a) OPNAVINST 5530.14C, *Navy Physical Security*, 10 Dec 98

(b) SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives,* 8 Oct 04

(c) SECNAV M-5210.1, *Records Management Manual,* Dec 05

(d) NTTP 1-01, *Naval Warfare Library,* Apr 05

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

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

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

(h) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

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

(j) SECNAVINST S5460.3C, *Management, Administration, Support, and Oversight of Special Access Programs within the DON (U)*, 5 Aug 99

(k) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI)*, 26 Jul 05

(l) SECNAVINST 5720.42F, *DON Freedom of Information Act (FOIA) Program*, 6 Jan 99

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

(n) OPNAVINST 5511.37C, *Nicknames, Exercise Terms and Code Words*, 22 Jul 97

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

(p) SECNAVINST 5510.30 (Series), *DON Personnel Security Program Regulation*

(q) SECNAVINST 3850.4, *Technical Surveillance Countermeasures (TSCM) Program*, 8 Dec 00

CHAPTER 8

DISSEMINATION

8-1 BASIC POLICY

1. Commanding officers shall establish procedures for the dissemination of classified and controlled unclassified information (CUI) originated or received by the 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 (also known as the "third agency rule").

3. Authority for disclosure of DON classified and CUI to foreign governments has been centralized in the Director, Navy International Programs Office, who has delegated authority to disclose certain classified information and CUI to those commands designated in reference (a). All such disclosures shall be accomplished in accordance with reference (a).

4. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, the Secretary of the Navy or a designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access. This shall be accomplished only under the following conditions:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

b. Limit the number of individuals who receive it;

c. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method per chapter 9 or other means deemed necessary when time is of the essence;

d. Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a

signed nondisclosure agreement; and

f. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

(1) A description of the disclosed information;

(2) To whom the information was disclosed;

(3) How the information was disclosed and transmitted;

(4) Reason for the emergency release;

(5) How the information is being safeguarded; and

(6) A description of the briefings provided and a copy of the nondisclosure agreements signed.

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, except as provided for in paragraph 8-1.4 above.

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 components and agencies within the executive branch of the U.S. Government, except as provided for in paragraph 8-1.4 above.

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 policy 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 policy and procedures for the dissemination of COMSEC information are contained in reference (f).

5. **SCI**. The policy and procedures for the dissemination of SCI are contained in reference (g).

6. **SIOP and SIOP-ESI**. The policy and procedures for the dissemination of SIOP and SIOP-ESI are contained in reference (h).

7. **NNPI**. The policy and procedures for the dissemination of classified and unclassified NNPI are contained in reference (i).

8. **FOUO**. The policy 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 provided that dissemination is not further controlled by a distribution statement. 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 6-11.3. The criteria for allowing access to FOUO Law Enforcement Sensitive information are the same as for FOUO information.

9. **SBU INFORMATION**. Per reference (j), the policy and procedures for the dissemination of SBU are the same as those used for FOUO information, except that information received from the Department of State marked SBU shall not be provided to any person who is not a U.S. citizen without approval of the Department of State activity that originated the information.

10. **DEA SENSITIVE INFORMATION**. Per reference (j), 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. **LIMITED DISTRIBUTION INFORMATION.** Unclassified information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by the National Geospatial-Intelligence Agency (NGA) to Military Departments or other DoD components for the conduct of official DoD business. Further dissemination outside DoD requires the express written approval of the Director, NGA, in accordance with reference (l).

8-5 DISSEMINATION OF INTELLIGENCE INFORMATION

Reference (m) provides the policy, control, and procedures for the dissemination and use of intelligence information and related materials.

8-6 DISSEMINATION TO CONGRESS

The policy 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 technical 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. Distribution statement assignments are usually made by second echelon commands with program responsibility.

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. 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 as 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 dissemination policy applies to all newly created technical documents to include engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or 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 (q) 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. This withholding authority does not apply to scientific, educational, or other data not directly and significantly related to design, production, or use in industrial processes.

8-8 PREPUBLICATION REVIEW

1. It is DoD policy under reference (r) that a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on publicly accessible websites or computer servers. Documents proposed for public release shall be first reviewed at the command level as required by reference (s) and may be found suitable for public release without higher-level consideration.

Commanders are authorized to release information to the public that is wholly within the command mission and scope. Each commanding officer is responsible for ensuring that a review of material proposed for public release is completed. This responsibility is normally delegated to the Public Affairs Officer. The security review is part of the overall public release process and is coordinated by the security manager in consultation with command subject matter experts.

2. If public release cannot be authorized within the chain of command, the material must be submitted for further review to the CNO (N09N2) or to the Commandant of the Marine Corps (ARS) (for Marine Corps matters). Exhibit 8B is an excerpt from reference (t) identifying official DoD information prepared by or for DoD personnel and proposed for public release that requires further review by the DoD Office of Security Review (OSR) via the CNO (N09N2). DoD OSR coordinates prepublication review with the cognizant authorities outside the DON and provides the final determination for public release.

REFERENCES

(a) SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives*, 8 Oct 04

(b) SECNAVINST S5460.3C, *Management, Administration, Support, and Oversight of Special Access Programs Within DON (U)*, 5 Aug 99

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

(d) SECNAVINST 5510.30 (Series), *DON Personnel Security Program Regulation*

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

(f) EKMS 1, *CMS Policy and Procedures for Navy Electronic Key Management System*, 5 Oct 04

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

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

(i) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 26 Jul 05

(j) DoD Regulation 5200.1R, *DoD Information Security Program Regulation,* 14 Jan 97

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

(l) DoD Directive 5030.59, *National Imagery and Mapping Agency (NIMA) LIMITED DISTRIBUTION Imagery or Geospatial Information and Data*, 13 May 2003

(m) DCID 6/6, *Security Controls on the Dissemination of Intelligence Information,* 11 Jul 2001

(n) SECNAVINST 5730.5H, *Mission, Functions, and Responsibilities of the Office of Legislative Affairs and Procedures for Handling Legislative Affairs and Congressional Relations*, 1 Sep 05

(o) OPNAVINST 5510.158A, *Security Review Guide for Congressional Matters*, 10 Dec 84

(p) DoD Directive 5230.24, *Distribution Statements on Technical Documents*, 18 Mar 87

(q) OPNAVINST 5510.161, *Withholding of Unclassified Technical Data from Public Disclosure*, 29 Jul 85

(r) DoD Directive 5230.9, *Clearance of DoD Information for Public Release*, 9 Apr 96

(s) SECNAVINST 5720.44B, *Department of the Navy Public Affairs Policy and Regulations*, 1 Nov 05

(t) DoD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release*, 6 Aug 99

EXHIBIT 8A

PROCEDURES FOR ASSIGNING DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS

1. Unclassified technical documents shall be assigned Distribution Statements A, B, C, D, E, F, or X. If assigning distribution statement A, the document must undergo public release approval prior to release.

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" below, in addition to Distribution Statement 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 recipients readily recognize it. For standard written or printed material, the distribution statement shall appear on the face of the document, title page, and SF 298, "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 SF 298, 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 Aug 1999 (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. 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 of determination). Other U.S. 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 policy manual or in the event the document is declassified.

(2) Reasons for assigning Distribution Statement B include:

(a) Foreign Government Information (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.

(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 of determination). Other U.S. 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 policy manual 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 the Department of Defense and U.S. DoD contractors only; (fill in reason) (date of determination). 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 policy manual 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 of determination). 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 policy manual 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 of determination) 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 6-11.2a.

(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; (date of determination). 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.

3. Unclassified documents that are marked with distribution statements B through X may also be marked "For Official Use Only." These documents are subject to withholding under the Freedom of Information Act, exemption (b)3.

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 DOD OFFICE OF SECURITY REVIEW PRIOR TO PUBLIC RELEASE

1. Certain categories of information require review and clearance by the DoD Office of Security Review via CNO (N09N2) before public release. They include information which:

a. Originates or is proposed for public release in the Washington, DC area. This requirement applies only to senior level personnel, e.g., flag officers and SES, on a politically or militarily sensitive topic;

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 authorized carriers transmit, transport, escort, or handcarry classified information. 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 be via government-to-government channels. Follow the provisions of exhibit 9A.

9-2 TOP SECRET

Transmit or transport U.S. Top Secret material only by:

1. Direct contact between appropriately cleared U.S. personnel;

2. The Defense Courier Service (DCS), if the material qualifies under the provisions of reference (a);

3. The Department of State (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 U.S. military or Government civilian personnel specifically designated to escort or handcarry the material, traveling on a private, public or Government owned, controlled, or chartered conveyance, or DoD contractor employee 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 U.S. owned 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. U.S. 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 holders of the General Services Administration (GSA) contracts for overnight domestic express delivery (see CNO (N90N2) web page at www.navysecurity.navy.mil for current listing). The sender shall verify the correct mailing address. The use of external (street-side) collection boxes is prohibited. These services are prohibited for weekend delivery. These carriers will not be used to transmit classified shipments to an air mobility command APOE of onward channel shipment to OCONUS destinations. 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; or

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 addressee’s 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 Surface Deployment Distribution Command (SDDC); or

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.** Reference (d) establishes the requirements for the transmission or transportation of COMSEC information.

2. **NATO**. Reference (e) 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 (f) establishes the requirements for the transmission or transportation of SCI.

4. **SAPs**. Reference (g) establishes the requirements for the transmission or transportation of SAP information.

5. **SIOP and SIOP-ESI.** Reference (h) establishes the requirements for the transmission or transportation of SIOP and SIOP-ESI.

6. **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 (i) establishes the requirements for the transmission or transportation of nuclear information or components.

7. **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 (j).

8. **NNPI.** The policies and procedures for the transmission or transportation of NNPI, U-NNPI, and DOE UCNI are contained in references (k) and (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) 140-2. (See the FIPS web page at www.csrc.nist.gov).

9. **SBU**. 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 (l).

12. **FOREIGN GOVERNMENT RESTRICTED AND UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE**. Per reference (m), 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 overheard by 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 holders of the GSA contracts 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.

9-10 RECEIPTING FOR CLASSIFIED INFORMATION AND FOREIGN GOVERNMENT 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 five years and Secret receipts for two years per reference (n)(see chapter 7, paragraph 7-8 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 classified material 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 unattended in vehicles, hotel rooms or hotel 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 office, in writing, of

the opening of the package;

i. Upon return, the courier shall return all classified material in a sealed package, with receipts for any information that is not returned; and

j. Refer to reference (e) 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 cognizant foreign disclosure authority shall ensure that disclosure authorization has been obtained per reference (m).

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, or a courier authorization letter. Any of these three written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or handcarry classified information (SAPs are excluded) between DoD commands subject to the following conditions:

a. The individual has a recurrent need to escort or handcarry classified information;

b. The expiration date may not exceed three years from the issue date (pertains only to DD 2501);

c. The written authorization is retrieved upon an individual's transfer, termination of employment, or when authorization is no longer required.

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.

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., Virginia 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. Letters should also include a valid U.S. Government telephone number for the command duty officer.

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. Senate regulations require that all classified material intended for delivery to any Senator, staff member, Committee or other Senate office be delivered to the Office of Senate Security (OSS) which is the central document control facility for the U.S. Senate. All Top Secret packages shall be handcarried to the OSS, Room S-407, the Capitol, Washington, DC 20510-7114.

2. Authorized couriers may also deliver Secret or Confidential packages directly to the following Committees:

a. The Committee on Appropriations, Room SD-122, Dirksen Building, United States Senate, Washington, DC 20510 (0900-1700 weekdays only);

b. The Committee on Armed Services, Room SR-228, Russell Building, United States Senate, Washington, DC 20510 (0930-1700 weekdays only);

c. The Committee on Foreign Relations, Room SD-415, Dirksen Building, United States Senate, Washington, DC 20510; or

d. The Committee on Intelligence, Room SH-211, Hart Building, United States Senate, Washington, DC 20510.

3. Secret or Confidential material that is sent by registered mail shall be sent to the OSS, even if intended for one of the four Committees cited above. In the event that authorized recipients at the above Committees are not available at the time delivery is attempted, classified material shall be delivered to the OSS. Each of the above Committees may only accept classified material addressed to and intended for the Chairman, Ranking Member, or a named staff member of the Committee. Under no circumstances shall classified packages be delivered directly to a Senator's personal office. OSS does not accept any classified material for the U.S. House of Representatives.

4. Prepare classified material 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*, 24 Jun 02

(b) USN/USMC Information Assurance Module IA 5239-22, *Protected Distribution Systems (PDS) Publication*, 1 Oct 03

(c) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Feb 05

(d) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

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

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

(g) SECNAVINST S5460.3C, *Management, Administration, Support, and Oversight of Special Access Programs within the DON (U)*, 5 Aug 99

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

(i) OPNAVINST C8126.1B, *Navy Nuclear Weapon Security (U)*, 14 Nov 02

(j) DoD 5200.1-R, *DOD Information Security Program,* 14 Jan 97

(k) NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI)*, 26 Jul 05

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

(m) SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives*, 8 Oct 04

(n) SECNAV M-5210.1, *Records Management Manual*, Dec 05

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.

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 policy manual, 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 (Surface Deployment and

Distribution Command (SDDC), 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 Cognizant Security Agency (CSA) 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 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 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 policy manual 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 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-008-8000

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 (N09N3)

REGISTERED NUMBER

SIGNATURE (Authorized Receipt)

R. L. WHEATON R L Wheaton

DATE 03/23/06

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 that is not being used or that is 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 pilferable 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 Director, Central Intelligence (DCI), for security containers used to store or process intelligence information.

4. Report to the Chief of Naval Operations (CNO (N3AT)), via CNO (N09N2), 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 policy manual, if applicable.

10-2 STANDARDS FOR STORAGE EQUIPMENT

The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, and associated security devices suitable for the storage and destruction of classified information. These are available at the DoD Lock Program site at: https://portal.navfac.navy.mil/portal/page?_pageid=181,4914415&_dad=portal&_schema=PORTAL. Reference (a) describes acquisition requirements for physical security

equipment used within the DoD. Reference (b) promulgates national policy for procuring and using security containers for Information Technology (IT) system purposes.

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; or

(d) Security-in-Depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740; or

(2) In a vault, modular vault or secure room constructed per exhibit 10A, equipped with an IDS and a personnel response 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) Until 1 October 2012, in a non-GSA-approved container having a built-in combination lock. One of the following supplemental controls is required:

(a) The location housing the security container is subject to continuous protection by cleared guard or duty personnel;

(b) A cleared guard or duty personnel shall inspect the area once every 4 hours; or

(c) An IDS with the personnel responding to the alarm within 15 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 2012.

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 (c) 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-L-2890 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 (d).

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. GSA approved containers are primarily used to store classified documents, components, materials, and equipment. There are several types and classes of GSA approved containers. Presently there are two classes of containers being manufactured: Class 5 and Class 6. Only Class 5 and 6 containers are on the current GSA schedule. Approved security containers removed from the GSA schedule 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.

3. GSA approved security containers and vault doors must have a GSA label affixed on the outside of the door or front of the control drawer (drawer with the combination lock). The label should have the words "GSA Approved Security Container" or "Vault Door" (as appropriate). If the container or vault door does not have the label, it may have been removed because the container/door is no longer approved. The container or vault door must be inspected and recertified by a person specifically trained and authorized by the GSA before it can be used to protect classified material. Upon completion of the inspection, a "GSA Approved Recertified Security Container" label will be applied and the container/vault door is then considered authorized for storage/protection of classified material. If the container fails inspection, it must be repaired in accordance

with Federal Standard 809, "Federal Standard Neutralization and Repair of GSA-Approved Security Containers," before the re-certification label can be applied. Information on availability and location of technicians may be obtained from the DOD Lock Program (800-982-1219) or from the GSA furniture center, www.gsa.gov.

4. GSA approved containers manufactured before October 1990 are identified by GSA label that has either black lettering on a silver background, or silver on black. Since October 1990 only Class 5, 6, and 7 containers have been manufactured. GSA approved Class 5 and 6 containers manufactured after October 1990 have a silver label with red lettering, or red with silver lettering. GSA approved Class 7 containers have a silver label with green lettering. Class 7 containers were available in filing cabinet style only and are no longer manufactured. New Information Processing System (IPS) containers are GSA-approved security containers for protection of IT systems. The labels for IPS have blue lettering.

a. Class 5 containers provide the same protection as Class 6 plus ten minutes against forced entry attack. Class 5 containers come in several types: file cabinet, map and plan, weapon storage, COMSEC, and IPS.

b. Class 6 containers are typically used for storage of classified information such as documents, maps, drawings, and plans. They come in file cabinet, and map and plan styles.

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, and beneath and between drawers.

10-6 SHIPBOARD CONTAINERS AND FILING CABINETS

1. Shipboard containers shall conform to DON standards for durability, size, weight, maintainability, and safety. 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. If the existing locks need repair or replacement, they will be replaced with locks meeting Federal Specification FF-L-2740.

2. The requirement to store Secret and Confidential information in these types of shipboard 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 designs shall include requirements for GSA-approved security containers and comply with the storage requirements of this policy manual.

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 control 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. 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 DECERTIFIED SECURITY CONTAINERS

1. Security containers manufactured by Remington Rand must be removed from service and disposed of under accepted safety standards.

2. Two and four-drawer Class 5 security containers manufactured by Art Metal Products, Inc., are no longer approved for the storage of classified information.

3. The GSA approval labels must be removed from decertified security containers.

10-10 RESIDENTIAL STORAGE

1. Top Secret information may not be removed from designated areas for work at home during off-duty hours except as authorized by the Secretary of Defense, the Secretaries of the Military Departments, the Combatant Commanders, or CNO (N09N).

2. Secret and Confidential information may not be removed from designated areas for work at home during off-duty hours except as authorized by the CNO (N09N), a Fleet Commander, 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 Forces Command.

3. These requests will not be considered unless a critical operational requirement exists. In each instance, commands shall develop written procedures that include the requirement for the information to be under personal control of the authorized individual at all times when it is not secured in a GSA-approved security container, identification and signature receipt of the information temporarily stored, and reconciliation upon its return. The classified information shall be stored in a GSA-approved storage container and protected by an IDS. Other methods of supplemental control may be used in lieu of an IDS, if they provide substantially the same assurance of protection.

4. A copy of all residential storage approvals shall be furnished to CNO (N09N2).

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 an 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 may not be repaired, but will be replaced with locks meeting Federal Specification FF-L-2740.

10-12 COMBINATIONS

1. Only personnel who have the responsibility and possess the appropriate security clearance eligibility and access will change combinations to security containers, vaults and secure rooms. Combinations will be changed:

a. When first placed in use;

b. When an individual knowing the combination no longer requires access unless other sufficient controls (e.g., security-in-depth) exist to prevent access to the lock;

c. When subjected to compromise; or

d. When taken out of service. Built-in combination locks will then be reset to the standard combination 50-25-50; combination padlocks will be reset to the standard combination 10-20-30.

2. In selecting combination numbers, sequential numbers (i.e., multiples of five, simple ascending or descending arithmetical series) and personal data, such as birthdates and Social Security numbers shall not be used. The same combination shall not be used for more than one container.

3. The classification of the combination shall be treated at the same level of the classified information stored therein. Mark any written record of the combination with the appropriate classification level.

4. Maintain a record for each security container, vault, or secure room door showing the location of each, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combinations and who are to be contacted in the event the security container, vault or secure room is found open and unattended. Use SF 700, "Security Container Information,"

for this purpose. 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 therein. Store Parts 2 and 2A in a security container other than the one to which it applies. If necessary, continue the listing of persons having knowledge of the combination on an attachment to Part 2.

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 will be equivalent to the highest classification level of information being protected by the padlock.

2. Reference (e) makes unauthorized possession of keys, key blanks, 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 (f) governs key security and lock control used to protect classified information.

10-14 SECURING SECURITY CONTAINERS

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

10-15 REPAIR, MAINTENANCE, AND OPERATING INSPECTIONS

1. Neutralization of lock-outs, repairs and maintenance of GSA-Approved security containers shall be accomplished in accordance with "Federal Standard 809, "Neutralization and Repair of GSA-approved Containers," and shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination per reference (g) 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 10-15.1.a(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. Go to the DoD Lock Program site for additional information.

2. GSA-approved containers that have been drilled in a location or repaired in a manner other than described in paragraph 10-15.1.a(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 "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 to indicate that 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, the locksmith should stamp a registration mark on the metal surface 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 or vault door per reference (h).

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. Intrusion Detection System (IDS).

    b. Closed Circuit Television (CCTV); and

    c. Access Control System (ACS).

2. An IDS consists of monitors and electronic sensors designed to detect, not prevent, an attempted intrusion. These sensors are designed to detect 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 imagers, switchers, and video motion detectors. An ACS system is designed to help control access to spaces. ACS components consist of card reader devices and/or biometrics, such as hand geometry, iris or fingerprint scanners, and the computers to control them.

3. An ESS provides additional protective controls at vital areas in the event of human or mechanical failure. The use of an ESS in the protection 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, its use may be justified as a more economical and efficient substitute for other protective measures.

4. 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 (h). 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 one day each year as "clean-out" day when specific attention and effort are focused on disposition of unneeded classified material. Classified material that cannot be destroyed because of its historical value shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

3. Refer to references (i) for destroying COMSEC information, reference (j) for destroying SCI, and reference (k) for destroying NATO information.

4. Refer to reference (l) for IT 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. 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 five square millimeters. New purchases of cross-cut shredders will be from those listed on the NSA/CSS Evaluated

Products List for High Security Crosscut Paper Shredders (see the latest information on cross-cut shredders at www.navysecurity.navy.mil). Crosscut shredders purchased prior to 1 January 2003 which reduce the information to shreds no greater than 3/64 inch wide by 1/2 inch long may continue to be used until October 2008; however, the bag containing the shredded material must be stirred or agitated prior to disposal.

3. Residue from disintegrators shall not exceed five square millimeters in size.

4. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

5. Strip shredders are not authorized for the destruction of classified information.

10-19 DESTRUCTION PROCEDURES

1. Commanding officers shall establish procedures to ensure that all classified material intended for destruction is destroyed by authorized means and appropriately cleared personnel.

2. Classified material pending destruction shall be controlled in a manner designed to minimize the possibility of unauthorized removal or access. A burn bag may be used to store classified material awaiting destruction at a central destruction facility. Seal and safeguard each burn bag at the highest level of classified material contained therein until actually destroyed.

3. A record of destruction is required for Top Secret information. OPNAV 5511/12, "Classified Material Destruction Report," may be used for this purpose. 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. Two witnesses shall sign the record when the information is placed in a burn bag or actually destroyed. Retain Top Secret records of destruction for five years as prescribed in reference (h). Records of destruction are not required for waste products. Top Secret working papers are not considered “waste products”.

4. Records of destruction are not required for Secret and Confidential information except for special types of classified

information (see paragraphs 7-8 and 10-17). Administrative procedures for recording final disposition of Secret material, whether by destruction or transmission outside the command, must be established in order to support the requirements of paragraph 7-4.

10-20 DESTRUCTION OF CONTROLLED UNCLASSIFIED INFORMATION

1. Destroy record copies of FOUO, SBU, DoD UCNI, DOE UCNI, and unclassified technical documents assigned Distribution Statements B through X, per reference (h). Non-record copies may be destroyed by any means approved for the destruction of classified information, or by any means that would make it difficult to recognize or reconstruct the information. Records of destruction are not required.

2. IT storage media containing digital FOUO, SBU, DoD UCNI, and unclassified technical documents shall, at a minimum, be reformatted prior to reuse within a DoD IT systems per references (l) and (m).

3. Destroy unclassified 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 (h) 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.

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 (n), 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 (n).

REFERENCES

(a) DoD Directive 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*, 17 Feb 89

(b) Committee on National Security Systems Policy (CNSSP) No. 10, *National Policy Governing Use of Approved Security Containers in Information System Security Applications,* 21 Jul 99

(c) OPNAVINST 5530.13C, *DON Physical Security Instruction for Conventional Arms, Ammunition and Explosives (AA&E)*, 26 Sep 03

(d) OPNAVINST 5112.6C, *Department of the Navy (DON) Postal Instructions,* 8 Jun 98

(e) Title 18, U.S.C., Section 1386, *Crimes and Criminal Procedures*

(f) OPNAVINST 5530.14C, *Navy Physical Security*, 10 Dec 98

(g) SECNAVINST 5510.30 (Series), *DON Personnel Security Program Regulation*

(h) SECNAV M-5210.1, *Records Management Manual*, Dec 05

(i) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

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

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

(l) DON IA Pub P-5239-26, *Remanance Security Guidebook*, May 00

(m) Assistant Secretary of Defense Memo, *Disposition of Unclassified DoD Computer Hard Drives*, 4 Jun 04

(n) SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives*, 8 Oct 04

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-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, metal, or other solid material 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 at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS either independently or by the motion detection sensors in the space.

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	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.)
[X] SECURITY CONTAINER [ ] VAULT DOOR	123456

MANUFACTURER: Mosler

GSA CLASS: [ ] ONE [ ] TWO [ ] THREE [X] FOUR [ ] FIVE [ ] SIX [ ] SEVEN

OPERATING PROBLEMS	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN NAME	TECHNICIAN ACTIVITY	ORGANIZATION NAME
Lockout	Neutralize	03/23/06	R. L. WHEATON	NCIS	NCIS

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION — **OPTIONAL FORM 89** (9-98)

OPERATING PROBLEMS	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN NAME	TECHNICIAN ACTIVITY	ORGANIZATION NAME

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION — **OPTIONAL FORM 89** (9-98) 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 enunciator 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 one 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 or 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 5510.30B.

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 5510.30B.

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(1) 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) Fingerprint

(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 command engages in classified procurement with U.S. industry, educational institutions or other cleared U.S. entities, both at the prime and sub-level, hereafter referred to as "contractors," or when cleared DoD contractors operate within areas under their direct control. Command security procedures shall include appropriate guidance, consistent with reference (a) and this policy manual, to ensure that classified information released to industry is safeguarded.

2. Commanding officers required to develop a Program Protection Plan in accordance with reference (b) shall levy these requirements on contractors via the contract.

11-2 AUTHORITY

1. Reference (c) established the National Industrial Security Program (NISP) for safeguarding information classified under references (d) or (e) that is released to industry. This policy manual implements the requirements of the NISP within the DON. Provisions of this policy manual relevant to operations of contractor employees entrusted with classified information shall be applied by contract or other legally binding instrument.

2. Reference (f) 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 (g) imposes requirements, restrictions, and safeguards necessary to protect special classes of information beyond those established in the baseline portion of reference (f).

4. Reference (h) establishes the authorities of the Intelligence Related Contracting Coordination Office and establishes policy and assigns responsibilities for the conduct of Intelligence Related Contracting within the DON in order to ensure the protection of sensitive intelligence and/or mission-related information during the acquisition process.

11-3 DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY MISSION

1. The Director of DSS oversees DoD implementation of the NISP through five regions comprised of field offices located throughout the U.S. Each region provides administrative assistance and policy guidance to local Field Offices charged with security oversight of contractors who perform on classified contracts. Consult the DSS Homepage at www.dss.mil for information pertaining to various DSS functions.

2. The Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio, processes and issues personnel and facility security clearances for contractors participating in the NISP; furnishes security assurances on U.S. contractor personnel and facilities to authorized foreign governments; reviews and processes visit requests for U.S. contractor employees to foreign government and contractor installations. It also responds to inquiries from defense contractors, military, Government agencies, DSS field elements and headquarters personnel who require information or assistance with individual clearance or investigative processing, to include Freedom of Information or Privacy Act requests and Congressional inquiries.

11-4 DSS AND COMMAND SECURITY OVERSIGHT OF CLEARED DoD CONTRACTOR OPERATIONS

1. **Shipboard**. On board ship, contractor employees have visitor status and shall conform to the requirements of this and command security regulations. Contractors shall submit written requests to the commanding officer who will then grant approval or disapproval for classified visits by employees to the ship.

2. **U.S. Shore Installations**. Contractors may perform work on and visit shore installations in one of the following ways:

a. When the commanding officer determines that the contractor is a short or long-term visitor, the commanding officer shall require that the visitor comply with command security regulations and shall be included in the command security education program.

b. When the contractor is a tenant aboard a U.S. installation, i.e., has sole occupancy of a facility or space controlled and occupied by the contractor, the host command may assume responsibility for security oversight over classified work carried out by the cleared DoD contractor employees in these facilities. The command is responsible for all security aspects of the contractor's operations in the facility. Oversight cannot be split between the commanding officer and

DSS. The contractor is considered a tenant and is obligated to comply with DON regulations and applicable portions of reference (f).

c. The commanding officer may request, in writing, that DSS grant the contractor an FCL and assume security oversight. If DSS accepts security oversight, DSS is responsible for all security aspects of the contractor operations. The commanding officer has no authority over the contractors' employees or its occupied spaces in this case. This process is normally used when a contractor is the sole occupant of a building or controlled space that it is leasing and/or managing the operation of on the shore facility.

3. **Off-Site Locations**. When contractors perform work at DON locations other than the command awarding the contract, the awarding command shall inform the new host of the contractual arrangement and forward a copy of the notification of contract award, a copy of the DD 254, and other pertinent documents to the host command.

4. **Overseas Locations**. Commands that award classified contracts requiring performance by contractors at DON overseas locations shall ensure that this policy manual is enforced in all aspects of contract security administration. The contractor and his or her employees shall be considered visitors and shall follow the security guidelines established by the host command. The host command shall furnish these requirements to the visitors; the awarding command shall provide to the host a copy of the contract, the DD 254 that describes the classified access authorized and other pertinent documents.

5. Command oversight of contractor employees working in DON spaces does not replace a company's other employee oversight responsibilities delineated in reference (f).

11-5 COR INDUSTRIAL SECURITY RESPONSIBILITIES

1. Paragraph 2-6 of chapter 2 identifies the appointment of a qualified security specialist as a Contracting Officer's Representative (COR). The following industrial security responsibilities are normally assigned to this COR. Other responsibilities may be required, as appropriate.

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, in coordination with the program manager, any additional security requirements, beyond those required by this policy manual, in the DD 254, or in the contract document itself.

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

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

f. Validate and endorse requests submitted by industry for Limited Access Authorizations for non-U.S. citizen employees. The endorsement must confirm that the appropriate foreign disclosure official has approved the release of the specified classified information. The request and its endorsement shall be forwarded to the Defense Security Service for processing the LAA investigation.

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

h. Review requests by contractors for retention of classified information beyond a two-year period and advise the contractor of disposition instructions or issue a final DD 254.

i. Ensure that timely notice of contract award is given to host commands when contractor performance is required at other locations and that Memoranda of Agreement (MOA) or Memoranda of Understanding (MOU) are in place to provide adequate security for the contractors.

11-6 CONTRACTOR FACILITY SECURITY CLEARANCES

1. Only a DON contracting command or cleared contractor (industry sponsor) may initiate an FCL process through DSS. Prime or higher-tier subcontractors initiate requests for classified subcontracts. Requests for FCLs must be based on a procurement requirement for a facility to have access to, or possession of, classified information. Requests shall be submitted to DSS and must contain the following information:

a. The name, address and phone number of the requester, including a point of contact.

b. The name, address (physical and mailing) and telephone number of the facility to be cleared, including the name of a facility official who shall serve as the point of contact during FCL processing.

c. The level of FCL required.

d. Justification for the request, including information regarding the nature of the tasks or services to be performed by the facility, contract number or copy of the DD 254, when possible.

e. Safeguarding requirements, if any.

2. If a contractor's FCL needs to be upgraded or revalidated, the cognizant contracting command shall submit a written request to DSS. Contractors, when eligible, are automatically granted Interim Secret or Confidential FCLs during processing of a final FCL. 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.

3. A DON command requiring an Interim Top Secret FCL for a contractor facility shall submit a request, in writing, to the DSS. 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. DISCO will take appropriate action and will notify the requesting command when action is completed.

11-7 PERSONNEL SECURITY CLEARANCE (PCL) UNDER THE NISP

1. An employee of a contractor granted an FCL under the NISP may be processed for a PCL when the contractor determines that access to classified information is essential to the performance of duty assignment. The PCL must be granted prior to an individual being given access to classified information. Personnel cannot be cleared for access to classified information at a higher level than the FCL of their employing contractor.

2. When there is no bona fide requirement for access to classified information in the performance of assigned duties, a PCL shall not be required. However, a requirement to conduct an investigation may still exist dependent upon the national security significance of the area or sensitivity of the information involved. In these cases, the contracting command may require that an investigation be conducted on contractor personnel in order to have some assurance that the employee is trustworthy and is eligible to perform sensitive duties. The investigative request must state that the investigation is for a trustworthiness determination. The contracting command shall include guidance in the contract for the contractor to request such investigations (see paragraph 11-16). Note that trustworthy investigations may be requested on either classified or wholly unclassified efforts.

11-8 DISCLOSURE OF CLASSIFIED INFORMATION TO A CONTRACTOR BY GOVERNMENT CONTRACTING AGENCIES

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, pre-contract 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 Central Verification Activity (CVA) maintains a database for each cleared facility which contains the FCL level and storage capability. The CVA updates the database with 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 at discofac@dislink.jcte.jcs.mil or at (1-888-282-7682) for verifications involving the storage of two cubic feet, or less, of classified information. Contractor storage capability involving the storage of over two cubic feet shall be verified directly with the cleared contractor. The CVA also maintains a database of cleared facilities at www.dss.mil; cleared contractors and U.S. government employees are eligible for access to the system. Follow the instructions provided at the site to obtain access.

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 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 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 DSS with notice of contract award, any special instructions (e.g., transmission, storage, and disposition instructions), and a copy of the DD 254.

d. Transmission or transportation of classified information to U.S. Government locations overseas shall comply with the requirements of chapter 9.

e. Execute, as necessary, an MOA or MOU with the host command to ensure that procedures are in place to provide adequate security for the contractors.

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 contracts with NATO activities or foreign governments under agreement with the U.S. The DSS will verify the security clearance and status of foreign contractor employees. Disclosure authority must be obtained from the cognizant foreign disclosure authority prior to releasing classified or controlled unclassified information to foreign contractors.

6. Restrictions on the release of information previously imposed by a competent authority govern in each case.

11-9 DISCLOSURE OF CONTROLLED UNCLASSIFIED INFORMATION TO A CONTRACTOR BY GOVERNMENT CONTRACTING AGENCIES

1. Contractors with a need-to-know may receive controlled unclassified information (CUI) consistent with the requirements of the contract unless there are restrictions on the release of the CUI to contractors.

2. A system exists within DoD to certify individuals and enterprises qualified to receive unclassified technical data with military or space application. These individuals and enterprises are referred to as Qualified Contractors. This certification is accomplished using a DD Form 2345, Militarily Critical Technical Data Agreement.

3. Upon receipt of a request under the Qualified Contractor program, 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). Releases shall be processed in accordance with reference (i).

4. Privately-owned or proprietary information provided by contractors, 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.

11-10 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).

11-11 VISITS BY CLEARED DoD CONTRACTOR EMPLOYEES

1. Classified information may be disclosed during visits provided the visitors possess appropriate PCLs and have a need-to-know for the classified information. The responsibility for determining need-to-know lies with the individual who will

disclose classified information during a visit.

2. DON contracting commands shall verify that visiting contractors have an FCL. Once the FCL of a contractor is established, a cleared contractor's certification of the clearance of an employee should be accepted. This certification could be by use of the visitor certification program in JPAS or a visit authorization request (VAR) from the contractor. Commands shall not accept a visit request handcarried by contractor personnel. Final approval of the visit is the prerogative of the commanding officer of the command to be visited. Reference (a) addresses visit requirements for contractor employees.

11-12 TRANSMISSION OR TRANSPORTATION

1. Appropriately cleared and designated DoD contractor employees may act as couriers, escorts, or handcarriers for classified information 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. The employee retains the 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 if there are overnight stops involved; and

d. The transmission or transportation meets all other requirements specified in chapter 9.

2. Appropriately cleared contractors may use the GSA-approved commercial contract carriers for overnight delivery of Secret and Confidential information to U.S. Government agencies within CONUS when procedures have been formally approved by the DSS prior to starting such transmissions (see reference (f)). GSA commercial carriers may not be used for Top Secret, COMSEC, NATO or foreign Government information.

3. If the methods specified in reference (f) cannot be used, the contracting command shall provide written authorization for the transmission of classified information to a U.S. Government

installation outside the U.S., Puerto Rico, or a U.S. possession or trust territory, if the contract does not already provide for such transmission.

11-13 RELEASE OF INTELLIGENCE TO CLEARED DOD CONTRACTORS

1. The Director, Office of Naval Intelligence (ONI) (ONI-5), 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. Appropriately cleared and access-approved contractors may receive intelligence information in support of a DON classified contract without prior approval from ONI-5 so long as access to intelligence is authorized in the contract (i.e., via the DD 254).

2. Prior to releasing intelligence to a cleared DoD contractor, the releasing command shall:

a. Ensure that dissemination is not prohibited by paragraph 11-17.

b. Ensure that the conditions of paragraph 11-17 are met.

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 the 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 to them, whether or not there is a Limited Access Authorization in place.

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.

6. Obtain the consent of the originator via the Director, ONI (ONI-5), prior to releasing to a cleared DoD contractor intelligence 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.

7. 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. Confirmation of need-to-know and a concise description of that portion of the contractor's study or project which will justify release of the requested intelligence information. This statement is a prerequisite for a release determination.

11-14 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).

11-15 FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)

1. It is the policy of the U.S. Government to allow foreign investment consistent with national security interests of the U.S. The FOCI policy for contractors is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to classified information. Foreign owned U.S. companies are NOT foreign companies. They are incorporated in the U.S. and are subject to U.S. laws and regulations, including the Arms Export Control Act and the Export Administration Act.

2. Notification of the possible acquisition of a cleared DoD contractor by a foreign government is provided by DSS to CNO (N09N2). What follows is a long process of identifying each DON procurement involved, notifying the affected commands, tasking them to evaluate the impact of a sale upon their programs, analyzing their input and making a preliminary determination of the contractor's value to the national interest. Should a final sale occur, the contractor is required to take actions to negate the FOCI using the approved methods allowable under the NISP: Voting Trust and Proxy Agreement; Board resolution; or Limited Facility Clearance (See Definitions).

3. If the contractor's proposal is rejected by DSS, the only remaining method to retain the services of the contractor is via a Special Security Agreement (SSA). An SSA is based on a recommendation by the cognizant contracting command that the services of the company are necessary to advance the national security interests of the United States. An SSA does not negate foreign ownership, but rather mitigates it. These contractors are permitted access to collateral Secret or Confidential information without additional action.

a. A contractor cleared under an SSA may not have access to proscribed information without a National Interest Determination (NID) by the listed cognizant authority:

(1) Top Secret information (CNO (N09N2));

(2) Communications Security (COMSEC) (except classified keys used to operate secure telephone units) (NSA);

(3) Restricted Data (RD) and Formerly Restricted Data (FRD) as defined by the Atomic Energy Act (DOE);

(4) Special Access Program (SAP) information (ODUSD (CI&S); and

(5) Sensitive Compartmented Information (SCI))(CIA).

b. A NID will state that release of the proscribed information will not harm the national security interests of the U.S., justify why the access is necessary, and explain why another cleared U.S. contractor cannot fulfill the requirement.

c. When a NID is required, it is the responsibility of the contracting command to submit a request to CNO (N09N2) for the proscribed information involved. CNO (N09N2) may approve access for certain proscribed information; if it does not have the authority to do so, it will then forward the request to the appropriate agency for approval.

d. When the sources of FOCI emanate from a country with which the DoD has signed a Declaration of Principles for Defense Equipment and Industrial Cooperation and that foreign government has agreed to oversee implementation of the SSA with the foreign parent, it is presumed that release of proscribed information to the U.S. contractor will not harm the national security and access limitations will not be imposed for DoD information. Consultation is required with CIA for SCI and DOE for RD and FRD.

4. A U.S. company determined to be under FOCI is ineligible for a FCL, and an existing FCL will be suspended or revoked unless security measures are taken to remove the possibility of unauthorized access or the adverse affect on classified contracts. Foreign ownership of a U.S. company under consideration for an FCL becomes a concern to the U.S. when a foreign shareholder has the ability, either directly or indirectly, whether exercised or exercisable, to control or influence the election or appointment of one or more members to

the applicant company's board of directors by any means. Foreign ownership which cannot be so manifested is not in and of itself, considered significant.

7. The U.S. Government reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

11-16 FACILITY ACCESS DETERMINATION (FAD) PROGRAM

1. The Internal Security Act of 1950 entrusts commanding officers to protect persons and property against the actions of untrustworthy persons. Reference (j) establishes 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.

2. When there is no bona fide requirement for access to classified information in the performance of assigned duties, a PCL will not be requested. The FAD program allows for trustworthiness investigations that do not meet the requirements for access to classified information. In such cases, the contracting command may require that an investigation be conducted on contractor personnel in order to have some assurance that an employee is trustworthy. Trustworthiness investigations are processed in accordance with reference (j). Investigative standards for contractor personnel requiring access to Information Technology (IT) systems with sensitive information are contained in reference (j).

3. Such determinations are outside the provisions of the NISP and the investigative request must state that the investigation is for a trustworthiness determination and the specific duty, function or situation that requires it. 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 sensitive services only. Reference (j) addresses specific requirements for administering the FAD program.

REFERENCES

(a) DoD 5220.22-R, *Industrial Security Regulation*, 4 Dec 85

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

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

(d) Executive Order 12958, as Amended, *Classified National Security Information*, 25 Mar 03

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

(f) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Feb 06

(g) DoD 5220.22-M.Supp 1, *National Industrial Security Program Operating Manual Supplement 1, (NISPOMSUP)* Feb 95

(h) SECNAVINST C4200.35, *Intelligence-Related Contracting (IRC) Within the Department of the Navy*, 1 Mar 01

(i) OPNAVINST 5510.161, *Withholding of Unclassified Technical Data from Public Disclosure*, 29 Jul 85

(j) SECNAVINST 5510.30B, *DON Personnel Security Program Regulation*

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 *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*
- [ ] a. ORIGINAL *(Complete date in all cases)* — DATE *(YYYYMMDD)*
- [ ] b. REVISED *(Supersedes all previous specs)* — REVISION NO. — DATE *(YYYYMMDD)*
- [ ] c. FINAL *(Complete Item 5 in all cases)* — DATE *(YYYYMMDD)*

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 classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Enter the Prime Contractor Here		Enter DSS Field Office or cognizant command

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	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Enter location where work is to be performed. If multiple, use block 13 or addendendum sheet		Enter DSS Field Office or cognizant command

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. CONTRACTOR 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 1999 PREVIOUS EDITION IS OBSOLETE.

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)*

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 classifiection 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.)*

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.

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 reference 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 provided to the contractor, either as attachments or under separate cover if they are classified. Requirements of the NISPOM should not be cited. 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.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [ ] Yes [ ] No
(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 in this item signifies that security requirements over and above those of the NISPOM will be imposed. Costs are normally reimbursed to the contractor.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [ ] No
(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 in this item relieves DSS of oversight of the contract.

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)*
R. L. Wheaton	Contracting Officer's Representative	COM (202) 433-4444 DSN 288-4444

d. ADDRESS *(Include Zip Code)*
Chief of Naval Operations (N09N2)
Washington Navy Yard, Building 176
Washington, D. C. 20388-5381

e. SIGNATURE
R L Wheaton

17. REQUIRED DISTRIBUTION
- [ ] a. CONTRACTOR
- [ ] b. SUBCONTRACTOR
- [ ] c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- [ ] d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- [ ] e. ADMINISTRATIVE CONTRACTING OFFICER
- [ ] f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

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 accounted for or physically located.

3. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid security clearance, authorized access or need-to-know.

4. A possible compromise occurs when classified information is not properly controlled.

5. For the purposes of this policy manual, electronic spillage occurs when data is placed on an IT system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this chapter.

12-2 REPORTING RESPONSIBILITIES

1. **Commanding Officer.** When a loss or compromise of classified information occurs, the cognizant commanding officer or security manager shall immediately initiate a Preliminary Inquiry (PI). If, during the conduct of the PI, it is determined that a loss or compromise of classified information did occur, the local NCIS office will be notified. The contacted NCIS office shall promptly advise whether or not it will open an investigation and provide advice and assistance to the PI as necessary. Timely referral to the NCIS is imperative to ensure preservation of evidence for any possible counterintelligence (CI) or criminal investigation.

2. **Security Manager.** The Security Manager shall be responsible for overseeing the PI. In the event of compromise or possible compromise on an IT system, the Security Manager shall coordinate

with the IA Manager (IAM) to ensure that these incidents are properly reported in accordance with both this policy manual and reference (a). Additionally, the IAM shall ensure that the possibly compromised classified information is sanitized from the affected system(s) in accordance with reference (e) when directed to do so by the security manager or commanding officer.

3. **Individual.** An individual who becomes aware that classified information is lost or compromised shall immediately notify their security manager or commanding officer of the incident, as well as their supervisory chain of command. If the reporting individual believes the security manager or commanding officer may be involved in the incident, they must notify the next higher echelon of command or supervision. If circumstances of discovery make such notification impractical, the reporting individual shall notify the commanding officer or security manager at the most readily available command or contact the local NCIS office.

12-3 PRELIMINARY INQUIRY

A PI is the initial process to determine the facts surrounding a possible loss or compromise of classified information. At the conclusion of the PI, a narrative of the PI findings will be prepared. This report will determine 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. This individual shall have security clearance eligibility and access commensurate to the classification level of the information involved; the ability to conduct an effective, unbiased investigation; and shall not be someone involved, either directly or indirectly, with the incident. The security manager shall provide advice and guidance, as necessary.

2. A PI shall be initiated and completed within **72 hours** of initial discovery of the incident. If circumstances exist that would delay the completion of the PI within 72 hours, the next superior in the administrative chain of command, the CNO (N09N2), the originator of the information, the Original Classification Authority (OCA) of the lost or compromised information, the local NCIS office and all others required by paragraph 12-8 shall be

notified of the reason for the delay and expected completion date. 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 of the information, 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). The PI shall identify the NCIS agent contacted, and also indicate whether a Judge Advocate General Manual (JAGMAN) investigation will or will not be conducted.

12-6 CLASSIFICATION OF THE PI MESSAGE OR LETTER

1. Every effort should be made to keep the PI unclassified and without enclosures. However, if the lost information is beyond the jurisdiction of the U.S. Government, and cannot be recovered, the PI shall be classified (using the classification and associated markings of the lost information as the derivative source) to prevent its recovery by unauthorized persons.

2. If the information involves a Public Media compromise and the PI contains information that could enable others to locate the classified information, the PI must be classified commensurate to the security classification level of the compromised information. See paragraph 12-18 for additional information on Public Media compromises.

12-7 ACTIONS TAKEN UPON PI CONCLUSION

1. Forward the PI by message or letter to the addressees in paragraph 12-4 if the PI concludes that a loss or compromise of classified information occurred or if a significant command security weakness or vulnerability is revealed. Loss or compromise should be assumed unless the information did not leave the control of the U.S. Government. A loss or compromise is

considered "beyond the jurisdiction of the U.S. Government" if the information is, for example, transmitted over the Internet; is publicly revealed or becomes the subject of a public media compromise; or is improperly revealed to an unauthorized individual or entity over which the U.S. Government has no authority.

2. A JAGMAN investigation is required in the event that disciplinary action is being considered or recommended by the PI, or compromise of classified information is considered likely to have occurred. In these circumstances, the command shall immediately initiate the JAGMAN investigation (see paragraphs 12-9 and 12-10), and notify the local NCIS office and all PI addressees. If the PI concludes that a significant security weakness or vulnerability exists due to the failure of a person to comply with established security practices and/or procedures, the commanding officer shall immediately take any necessary corrective actions to prevent recurrence.

3. Do not forward 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 due to the belief that the information was never outside the control of cleared U.S. Government personnel. However, if minor security weaknesses or vulnerabilities are revealed due to the failure of a person to comply with established security practices and/or procedures, the commanding officer will immediately take the necessary disciplinary and/or corrective actions to prevent recurrence.

4. A record of the PI must be kept regardless of its conclusions. If the PI concludes that further action is not warranted, and the report is not to be forwarded per paragraph 12-4, the PI may be recorded as a memorandum for the record or other less formal document. Such records will be retained for two years per reference (b).

5. Determining the course of action at the conclusion of a PI remains the responsibility of the commanding officer, who must carefully consider the circumstances surrounding each loss or compromise, and apply risk management principles in making decisions about the probability of compromise. The security manager shall provide advice and guidance to the commanding officer, as appropriate, in making this decision. Additionally, the security manager will take appropriate administrative action regarding any individual's failure to comply with established security practices.

12-8 REPORTING LOSSES OR COMPROMISES OF SPECIAL TYPES OF CLASSIFIED INFORMATION AND EQUIPMENT

1. Report losses or compromises of classified IT systems, terminals, or equipment to the CNO (N09N2). The CNO (N09N2) shall notify CNO (N6) and the Director, Information Assurance, Undersecretary of Defense (Intelligence).

2. Report losses or compromises involving NATO classified information to CNO (N09N2). Per reference (a), CNO (N09N2) will notify the Navy International Program Office (IPO) and the United States Security Authority for NATO affairs (USSAN) via the Office of the Deputy Undersecretary of Defense (TSP&NDP).

3. Report losses or compromises involving FGI to the CNO (N09N2), who shall notify ODUSD (TSP&NDP).

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(CI&S)) via the Director, Special Programs Division (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), who shall notify the Department of Energy, with a copy to the local NCIS office.

6. Report losses or compromises involving SIOP and SIOP-ESI to the Joint Chiefs of Staff (JCS) and the U.S. Commander, Strategic Command (USSTRATCOM) by the quickest means possible, consistent with security requirements. Include an opinion as to the probability of compromise. The USSTRATCOM commander 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, which shall determine if a traffic review is necessary. If a review is warranted, it shall be conducted using the procedures contained in reference (c). The "initial report" required by reference (c) satisfies the requirement for a PI (see paragraph 12-2), provided copies are sent to CNO (N09N2), the National Security Agency, 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 (d).

9. Report losses or compromises of classified information which involve other Government agencies to the Office of the Deputy Undersecretary of Defense (Counterintelligence and Security) (ODUSD (CI&S)) via CNO N09N2.

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.

11. The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DoD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

12-9 JAGMAN INVESTIGATIONS

1. A JAGMAN investigation is an administrative proceeding conducted per chapter II of reference (e). A JAGMAN investigation is 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 disciplinary action or additional corrective action.

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 Office of the Judge Advocate General (OJAG) (Code 17). Whenever a violation of criminal law appears to have occurred and criminal prosecution is contemplated, the OJAG (Code 17) shall notify the DON General Counsel.

3. Designation as a national security case (see reference (e)) 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 security clearance eligibility and access commensurate to the classification level of the information involved; the ability to conduct an effective, unbiased investigation; and shall not be someone involved, either directly or indirectly, with the incident. The command security manager may not be appointed to conduct the JAGMAN investigation, but may provide advice and guidance to the investigating official (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 by paragraphs 12-3 and 12-8 will 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 or the nearest Trial Service Office. This format is merely a guideline; the final JAGMAN should, at a minimum, contain the information shown in the example.

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 NCIS initially declined investigative action. For example, 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. NCIS ROIs are exempt from certain disclosure provisions of reference (f), while JAGMAN investigations are not. By attaching the NCIS ROI to the JAGMAN investigation, the ROI loses its exempt status and may be disclosed in total under reference (f). Extracts or statements acquired through the NCIS ROI may be used in findings of fact, but their use must 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 (f).

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 and the originator and the OCA of the compromised information. If the originator or the OCA is assigned to the office of the CNO or a command outside the DoD, the CNO (N09N2) will 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 the JAGMAN investigation for completeness and return any deficient JAGMAN investigation for additional investigation or corrective action. If the immediate superior is involved in the incident under investigation, then the JAGMAN must be forwarded to the next higher chain of command for endorsement. 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 to prevent similar incidents is very important

and shall be specifically addressed.

c. Determine whether security practices are in conflict with this policy manual and if they are being corrected.

d. State and review the disciplinary action 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, an explanation must be provided. Affirm that the command will comply with reference (g) concerning continuing evaluation of the responsible individual's eligibility for access to classified information.

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 shall 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 that person is 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 it was subjected to compromise.

c. Whether further review is required by another DON or DOD activity, or Executive Branch agency.

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 and modify applicable security classification guides in accordance with reference (h).

12-17 DAMAGE ASSESSMENTS

A damage assessment is a multi-disciplinary analysis to determine the effect of a compromise of classified information on 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. A formal damage assessment is not to be confused with the reviews conducted by the command or OCA regarding classification and programmatic impact, or with the classification review performed in support of a prosecution. Depending upon the circumstances of the compromise, a formal damage assessment is not always necessary.

12-18 PUBLIC MEDIA COMPROMISES

1. A public media compromise is the unofficial release of DoD classified information to the public resulting in its unauthorized disclosure.

2. When an individual or command becomes aware that classified 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 is taken. Upon notification of a compromise through the public media, the CNO (N09N2) shall consult with the Chief of Navy of Information (CHINFO), the Assistant Secretary of Defense (Public Affairs), NCIS, and 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 to the NCIS;

c. If the information is, or appears to be, under the cognizance of another DoD component, forward the case to the ODUSD (CI&S), 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. NCIS shall:

a. Promptly initiate an investigation, if warranted, and prepare a summary of the investigation and forward it to the ODUSD (CI&S), via the CNO (N09N2);

b. Provide assistance to the ODUSD (CI&S), 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 is taken, that fact shall be recorded.

12-19 INCIDENTS INVOLVING IMPROPER TRANSMISSIONS

Any command that receives classified information that has been 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, Internet, or posted to a publicly accessible and/or unencrypted website). 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). Security Discrepancy Notices for shall be retrained for two years.

REFERENCES

(a) DON Information Assurance (IA) Publication 5239-26 *Remanence Security Guidebook*, May 2000

(b) SECNAV M-5210, *Records Management Manual*, Dec 05

(c) EKMS-1, *CMS Policy and Procedures for Navy Electronic Key Management Systems (U)*, 5 Oct 04

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

(e) JAGINST 5800.7D, *Manual of the Judge Advocate General*, 22 Mar 04

(f) Title 5, U.S.C., Section 552a, *The Privacy Act of 1974*

(g) SECNAVINST 5510.30B, *DON Personnel Security Program Regulation*

(h) OPNAVINST 5513.1F, *DON Security Classification Guides*, 7 Dec 05

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

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 5510.36A
(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**: (DATE OF DOCUMENT)

(4) **ORIGINATOR**:

(5) **OCA(S)**: OCA NAME, CONTACT INFORMATION AND GUIDANCE PROVIDED BY OCA.

(6) **SUBJECT OR TITLE**:

(7) **DOWNGRADING/DECLASSIFICATION INSTRUCTIONS**:

Subj: PRELIMINARY INQUIRY (PI)

(8) **NUMBER OF PAGES OR ITEMS OF EQUIPMENT INVOLVED:**

(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:** (Indicate when NCIS was notified, the name and phone number of the agent contacted, and if NCIS accepted or declined investigative jurisdiction.)

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) CONTEMPLATED:** (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;

Subj: PRELIMINARY INQUIRY (PI)

d. A loss or compromise of classified information may have occurred due to a significant command security weakness(es) or vulnerability(ies); or

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; if incident occurred on an IT system, indicate how the affected system(s) was sanitized).

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 5510.36A//
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: (DATE OF THE DOCUMENT)
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, SA NOTIFIED AND TELEPHONE NUMBER. 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) CONTEMPLATED: (IF ANY).

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) WAS 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. IF INCIDENT OCCURRED ON AN IT SYSTEM, INDICATE HOW THE SYSTEM WAS SANITIZED.).

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) (Preliminary inquiry should be provided as an enclosure; other enclosures as necessary).

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**: (The date of document).

d. **ORIGINATOR**:

e. **OCA(S)**: (Identity of OCA, date contacted and guidance provided).

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 what action NCIS took 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 shall be classified at the same level as the lost information or equipment; this report will be classified since it will identify this information.

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 as determined by the initial security review or the classification review by the cognizant OCA. Provide any supporting data for your conclusions(s).

Subj: JAGMAN INVESTIGATION FORMAT

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).

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 (loss of control of 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 FOR 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

FROM (Originating command) | DATE

REF a. SECNAVINST 5510.36 (series) *(Insert ref. (a))* b. OPNAVINST 5510.1 SERIES

ENCL

TO: (Forwarding command)

(Note - This form may be mailed in a window envelope.)

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 UNAUTHORIZED		DOWN GRADING DATA INCORRECT		DECLASSIFICATION (OR REVIEW) DATA OMITTED OR INCORRECT

OTHER *(Specify)*

Fold here ↑ with face of form in view

COMMENTS *(Continue on reverse, if necessary)*

COPY TO: N-009D (WITH ADDRESSEE DELETED)

SIGNATURE | TITLE

OPNAV 5511/51 (MAY 1980) This form replaces OPNAV 5511/8; 22 and 24 which are obsolete. Page 1 of 2 Pages

APPENDIX A

DEFINITIONS AND ABBREVIATIONS

Access - The ability and opportunity to obtain knowledge or possession of classified information.

Acquisition Systems Protection (ASP) - A program designed to identify and protect 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.

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 as well as the Defense Intelligence Agency, the National Security Agency and the National Reconnaissance Office.

Alternative Compensatory Control Measures (ACCM) – Used when an Original Classification Authority (OCA) determines that other security measures (as detailed in this instruction) are insufficient for establishing "need-to-know" for classified information, and where Special Access Program (SAP) controls are not warranted. The purpose of ACCM is to strictly enforce the "need-to-know" principle.

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.

Authorized Person – A person who has a need-to-know for the specified classified information in the performance of official duties and who has been granted an eligibility determination at the required level

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 frame

for duration of classification established under E.O. 12958, as Amended.

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.

Caution-Proprietary Information Involved (PROPIN) - Intelligence control marking used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value.

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, as Amended, 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 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) - An office functioning on behalf of the Cognizant Security Agency responsible for establishing an industrial security program for the purpose of safeguarding classified information disclosed or released to U.S. industry. A CSO is designated for each contract issued by the Cognizant Security Agency.

Collateral Information - Information identified as NSI under the provisions of E.O. 12958, as Amended, 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 officer, 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 issue 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 telecommunication systems (See definition for EKMS).

Compromise - An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.

Confidential – A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security, that the OCA is able to identify or describe (E.O. 12598, as Amended).

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 SDDC to transport classified 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 as 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 Officer's Security Representative).

Controlled Cryptographic Item - A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified when un-keyed (or when keyed with unclassified key) but controlled.

Controlled Unclassified Information (CUI) - Official information not classified or protected under E.O. 12958, as Amended, 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 that 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.

Dissemination and Extraction of Information Controlled by the Originator (ORCON) – Most restrictive intelligence control marking used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination.

Disclosure - Conveying classified information to another person.

Distribution Controlled Information – Classified or unclassified information assigned distribution statements by the generating and/or responsible organizations to determine its distribution availability.

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.

Duration of Classification – A specific date or event, as established by the original classification authority, for automatic declassification of information based upon the duration of the national security sensitivity of that information as established by E.O. 12598, as Amended.

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 (12 months or longer) or permanent deviation from a specific safeguarding requirement of this regulation. Exceptions require compensatory security measures.

Electronic Key Management System (EKMS)- Consists of four tiers designed to provide an integrated, end-to-end key management, and Communications Security (COMSEC) material generation, distribution, and accounting system for the Department of Defense (DoD) and civilian agencies.

Electronic Media – Used on Information Technology Systems to store or transfer information (i.e., Universal Serial Bus drives, flash drives, thumb drives, pen drives, compact disks, scanners, videotapes, floppy disks, recordings, etc.).

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.

For Official Use Only (FOUO) – A marking applied to unclassified information that meets one or more exemptions of the Freedom of Information Act (FOIA) under Title 5 U.S.C., Section 522 (b) (2) through (9). Information must be unclassified to be designated FOUO. Declassified information may be designated FOUO, if it qualifies under exemptions 5 U.S.C. 522 (b)(2) through (9).

For Official Use Only Law Enforcement Sensitive (FOUO-LES) – A marking applied to unclassified information that meets one or more exemptions of the Freedom of Information Act (FOIA) under Title 5 U.S.C., Section 522 (b)(2) through (9). It is intended to denote that the information was compiled for law enforcement purposes.

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, as Amended.

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.

Immigrant Alien - Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Industrial Security - That portion of information security that 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, as Amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Manager (IAM) - Responsible for the information assurance program for a DON information system or organization. This individual is responsible for creating the site accreditation package. The IAM functions as the Command's focal point on behalf of and principal advisor for IA matters to the Designated Approving Authority (DAA). The IAM reports to the DAA and implements the overall IA program. Previously called the Information Systems Security Manager (ISSM) and ADP Systems Security Officer (ADPSSO).

Information Assurance Officer (IAO) - Implements and enforces system-level IA controls in accordance with program and policy guidance. Previously called the Information Systems Security Officer (ISSO).

Information Technology System – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception data or information. This includes computers, ancillary equipment, software and firmware.

Infraction - Any knowing, willful, or negligent action contrary to the requirements of E.O. 12958, as Amended, 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 the DSS Facility Clearance Branch following authorization by a U.S. Government activity to avoid crucial delays in pre-contract 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 that has been compromised or subjected to compromise.

Limited Distribution – A caveat used only by the National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NGA or information, data and

products derived from such information.

Mandatory Declassification Review - Review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.5 of E.O. 12958, as Amended.

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, as Amended, 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, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and 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, assigned an unclassified meaning that is employed for unclassified, administrative, morale, or public information purposes.

Not Releasable to Foreign Nationals (NOFORN) – An intelligence control marking used to identify intelligence which an originator has determined falls under the criteria of DCID 6/7, and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

North Atlantic Treaty Organization (NATO) – A military alliance of 26 countries from North America and Europe.

Official Information - Information that is owned by, produced for or by, or is subject to the control of the U.S. Government.

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."

Patent Secrecy Act – Protection of information in which the U.S. Government has a property interest that if published (i.e., an application or the granting of a patent) might be detrimental to the national security. It is governed by Title 35 U.S.C., Section 181.

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 (including 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, Northern Mariana Islands, Wake Island, and Palmyra Atoll.

Preliminary Inquiry (PI) - The "initial" process to determine the facts surrounding a possible loss or compromise. A narrative of the PI findings is required when there is a loss or compromise of classified information. All preliminary inquiries

must be documented for record purposes.

Program Manager – Designated senior level official responsible for managing all aspects of development, production, sustainment and delivery related to an acquisition program. Develops program strategies and identifies industry roles and requirements in support of their programs.

Program Protection Plan (PPP) - The PPP is the program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to Critical Program Information to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access.

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 SDDC 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.

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.

***R*etrieval and *A*nalysis of *N*avy *K*(C)lassified *IN*formation (RANKIN) PROGRAM –** Provides for the standardization, centralized management, and issuance of all DON security classification guides (SCGs) and maintenance of historical files for all DON SCGs.

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.

Secret - A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, that the OCA is able to identify or describe (E.O. 12598, as Amended).

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 that 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, as Amended, and its implementing directives.

Senior Agency Official (SAO) - The official designated by the agency head under section 5.4(d) of E.O. 12958, as Amended, 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 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(CNO N5 GP2).

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, as Amended) 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.

Spillage – Occurs when data is placed on an IT system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this instruction.

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.

Tentative Classification - Allows those individuals without original classification authority, who create information they believe to be classified or which they have significant doubt about the appropriate classification, to mark the information accordingly.

Top Secret - A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, that the OCA is able to identify or describe (E.O. 12598, as Amended).

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 Puerto Rico, and those possessions listed in the definition above.

U.S. Citizens (including U.S. Nationals) - A person born in the United States or any of its territories, a person born abroad but having one or both parents who are themselves United States citizens, and a person who has met the requirements for citizenship as determined by the Immigration and Naturalization Service and has taken the requisite oath of allegiance.

U.S. Person - A U.S. citizen or a natural person who is a lawful permanent resident as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state or local), entity.

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.

Working Papers - Documents and material accumulated or created while preparing finished material (e.g., classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents).

ABBREVIATIONS

ACCM – Alternative Compensatory Control Measures

ACS - Access Control System

AEA - Atomic Energy Act

AECS - Access Entry Control Systems

ASP - Acquisition Systems Protection

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

COMSEC - Communications Security

CONUS – Continental United States

COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)

CSA - Cognizant Security Agency

CSO - Cognizant Security Office

CSP - Cryptographic Security Publication

CSS - Constant Surveillance Service

CUI – Controlled Unclassified Information

CUSR - Central U.S. Registry (NATO)

CVA - Central Verification Activity

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

DHS – Department of Homeland Security

DLSC - Defense Logistics Services Center

DNI - Director of Naval Intelligence

DoD - Department of Defense

DOE - Department of Energy

DON CIO – Department of the Navy Chief Information Officer

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

DUSD(CI&S) - Deputy Under Secretary of Defense for Counterintelligence and Security)

DUSD(TSP&NDP) - Deputy Undersecretary of Defense for Technology Security Policy and National Disclosure Policy)

EKMS – Electronic Key Management System

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

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

FOUO LES – For Official Use Only Law Enforcement Sensitive

FRD - Formerly Restricted Data

GAO - General Accounting Office

GSA - General Services Administration

IA – Information Assurance

IC - Intelligence Community

IDE - Intrusion Detection Equipment

IDS - Intrusion Detection Systems

IR&D - Independent Research and Development

ISP - Information Security Program

ISCAP – Interagency Security Classification Appeals Panel

ISOO - Information Security Oversight Office

IAM - Information Assurance Manager

IAO - Information Assurance Officer

ITAR - International Traffic in Arms Regulation

IT – Information Technology

JAG - Judge Advocate General of the Navy

JAGMAN – Judge Advocate General Manual

JANAP - Joint Army, Navy, Air Force Publication

JCS - Joint Chiefs of Staff

LAA - Limited Access Authorization

LIMDIS – Limited Distribution

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

NETWARCOM SD – Naval Network Warfare Command Security Directorate

NGA – National Geospatial-Intelligence 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

NSI – National Security Information

NSN - National Stock Number

NWP - Naval Warfare Publication

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

OSD - Office of the Secretary of Defense

OSR – Office of Security Reviews (DoD)

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

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

SDDC - Surface Deployment Distribution Command

SECDEF - Secretary of Defense

SECNAV - Secretary of the Navy

SF - Standard Form

SIOP - Single Integrated Operational 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

USD(I) – Under Secretary of Defense for Intelligence

USD(P) - Under Secretary of Defense for Policy

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 (12-99) Contract Security Classification Specification	0102-LF-011-5800
DD 2501 (3-88) Courier Authorization Card	0102-LF-000-6900
OPNAV 5511/10 (12-89) Record of Receipt	0107-LF-008-8000
OPNAV 5511/51 (5-80) Security Discrepancy Notice	0107-LF-055-5355

These forms are available only through GSA.

SF 700 (4-01) Security Container Information	7540-01-214-5372
SF 701 (8-85) Activity Security Checklist	7540-01-213-7899
SF 702 (8-85) Security container Check Sheet	7540-01-213-7900
SF 703 (8-85) Top Secret Cover Sheet	7540-01-213-7901
SF 704 (8-85) Secret Cover Sheet	7540-01-213-7902
SF 705 (8-85) Confidential Cover Sheet	7540-01-213-7903
SF 706 (1-87) Top Secret Label	7540-01-207-5536

SF 707 (1-87) Secret Label	7540-01-207-5537
SF 708 (1-87) Confidential Label	7540-01-207-5538
SF 709 (1-87) Classified Label	7540-01-207-5540
SF 710 (1-87) Unclassified Label	7540-01-207-5539
SF 711 (1-87) Data Descriptor Label	7540-01-207-5541
SF 712 (10-87) Classified SCI	7540-01-267-1158
OF 89 (9-98) Maintenance Record for Security Containers/Vaults	Local reproduction 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)	Exh 2B-2
Agency Security Classification Management Program Data	SF-311	1-2

TABLE OF REVISIONS/CHANGES

SECNAV Manual	Basic Instruction Date
M-5510.36	June 2006

Change Number	Revision Date

BRIEF OF REVISIONS/CHANGES

The following are major changes in policy and procedures incorporated in the last revision to this SECNAV Manual. A revised Foreword and Table of Contents will be issued with each change.

1. Chapter_____, Page_____, Paragraph_____:

2. Chapter_____, Page_____, Paragraph_____:

3. Chapter_____, Page_____, Paragraph_____:

4. Chapter_____, Page_____, Paragraph_____:

5. Chapter_____, Page_____, Paragraph_____:

6. Chapter_____, Page_____, Paragraph_____:

7. Chapter_____, Page_____, Paragraph_____:

8. Chapter_____, Page_____, Paragraph_____:

9. Chapter_____, Page_____, Paragraph_____:

10. Chapter_____, Page_____, Paragraph_____:

STOCK NUMBER
0516LP1055279