CHAPTER 9

SECURITY

LEARNING OBJECTIVES

Upon completion of this chapter, you should be able to do the following:

1. Recognize the Navy policy for training personnel in the content of the U.S. Navy Information and Personnel Security Program.

Security violations discovered at various military and government establishments worldwide reveal a need to upgrade the security awareness of every service member. Consider the tragedies that have occurred to our diplomatic corps, military personnel, and other officials over the past several years. Many of these tragedies can be directly attributed to a lack of security, a lack of security education, or lax security measures. As you advance in rate, your knowledge of security measures and the security education of your personnel increasingly affect the security of your command.

This chapter begins with an explanation of the Naval Information and Personnel Security Program. It outlines the basic policies and security procedures involved in management of the program.

Next the chapter explains classified materials and the assignment of classified material designations. It covers the different types of restricted areas used to safeguard and store classified materials and the amount of security needed in each area. *Department of the Navy Information and Personnel Security Program Regulation* provides detailed procedures for the safeguarding and proper storage of classified materials.

The chapter concludes with discussions of personnel-security clearances, access to classified materials, and automatic data processing (ADP) security. It explains the different types of clearances and the required investigations for each clearance. It also discusses the guidelines for the Personnel Reliability Program. This program impacts on every command that is nuclear powered or has nuclear weapons capability. If the program is not properly administrated, it can have a devastating effect on the security of your command and its ability to perform its assigned mission. Remember—only YOU can be responsible for the security and protection of your country.

Although this chapter deals chiefly with the security of classified materials, you can apply the basic concepts to other areas to increase security within your command.

THE DEPARTMENT OF THE NAVY INFORMATION AND PERSONNEL SECURITY PROGRAM

The Information and Personnel Security Program safeguards the disclosure of classified information and materials to unauthorized persons. The following persons must comply with the basic policies of this program:

- Navy and Marine Corps personnel (active-duty and Reserve)
- Other armed services members assigned to a Navy or Marine Corps unit or installation
- Civilian employees of the federal government, including employees of the Office of Personnel Management (OPM), as well as civilian contract employees

BASIC POLICY

The Information and Personnel Security Program protects national security in two basic areas. First, it monitors security in the appointment or retention of Department of the Navy civilian employees. Second, it oversees security in the acceptance or retention of Navy or Marine Corps personnel. The program also ensures the national security when personnel are granted access to classified information or are assigned to other sensitive duties. Access to classified information is granted on a strict, need-to-know basis.

Authority

The Secretary of the Navy is responsible for setting up and maintaining an Information Security Program and a Personnel Security Program. The Secretary of the Navy has made the Chief of Naval Operations responsible for information and personnel security. The Special Assistant for Naval Security and Investigative Matters who carries the Chief of Naval Operation (CNO) staff code OP-09N ensures the effectiveness of the security program. OP-09N also serves as the Commander, Naval Security and Investigative Command (COMNAVSECINVCOM). COMNAVSECINVCOM devises information and personnel security policies and procedures based on directives from higher authority and issues directives for the program. Under the Director of Naval Intelligence, CNO (OP-092), the Commander, Naval Intelligence Command, administers the sensitive compartmented information (SCI) system for the Navy.

The *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1H, contains COMNAVSECINVCOM guidelines. Those guidelines serve as the minimum requirements for management of the program. Commanding officers may impose more stringent requirements within their own commands. However, they may not establish requirements that are contradictory to OPNAVINST 5510.1H.

Program Management

The National Security Council (NSC) provides overall policy guidance on information and personnel security. The Director, Information Security Oversight Office (ISOO), has responsibility for setting up and monitoring the security program for classified information. The ISOO may request information or materials from the Department of the Navy when an organization needs that information to perform its functions.

The Office of Personnel Management prescribes the requirements (including investigations) for civilian government employment.

The Director of Central Intelligence (DCI) serves as the chairman of the National Foreign Intelligence Board. As chairman, the DCI issues instructions affecting intelligence policies and activities. These instructions are based on Director of Central Intelligence directives (DCIDs) or Director of Central Intelligence policy statements.

The Federal Bureau of Investigation (FBI) is the chief internal security agency of the federal government. It has jurisdiction over more than 170 different investigative matters, which include espionage, sabotage, treason, and other subversive activities. The Naval Investigative Service is the Department of the Navy's sole liaison with the FBI on internal security matters.

The CNO office (OP-09N) serves as the liaison about information and personnel security matters between the Department of the Navy and the Office of the Secretary of Defense. The CNO office also serves as the liaison between the Department of the Navy and other components of the Department of Defense and other federal agencies.

The following is a list of organizations with which OP-09N has a close security relationship:

Headquarters, Marine Corps, Naval Military Personnel Command and Naval Civilian Personnel Command in their responsibilities for administering personnel security

Naval Intelligence Command (NIC-04) in its responsibility for the management of the sensitive compartmented information (SCI)

Naval Security Group Command in its responsibility for the security and administration of SCI programs

The Commander, Naval Security and Investigative Command (COMNAVSECINVCOM), is responsible for the Department of the Navy's investigative, law enforcement, counterintelligence, and physical security policies and programs. (However, COMNAVSECINVCOM is not responsible for the physical protection of classified materials.) The Naval Investigative Service supports COMNAVSECINVCOM in these responsibilities.

Command Security Procedures

If your command handles classified information, it prepares and keeps current written command security procedures. The procedures specify how the command is to accomplish the requirements of OPNAVINST 5510.1H.

The command's security procedures cover what will be done, who will do it, and who will supervise it. General statements, such as "Secret material will be accounted for using OPNAVINST 5510.lH," do not satisfy this requirement. The written procedures must be specific, based on the OPNAVINST 5510.1H requirements that apply to your command.

Your command may not be involved with all phases of the Information and Personnel Security program. However, all commands share some elements in the security of classified information. They all follow security procedures in the accounting and control, physical security, reproduction, and destruction of classified materials. All take security measures in granting and recording access to classified materials and the control of visitors to classified areas. All ensure the proper classification, marking, downgrading, and declassification of classified materials. In addition, all must provide security education.

Responsibility for Compliance

The commanding officer is responsible for the effective management of the Department of the Navy Information and Personnel Security Program within the command. Every person, military or civilian, in the Navy and Marine Corps is responsible for obeying the *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.lH.

Command Management

Command security management, discussed in the following paragraphs, includes the following responsibilities:

1. Designating a security manager
2. Designating a Top Secret control officer if the command handles Top Secret information
3. Designating an ADP security officer (or Information Systems security officer) if the command is involved in processing data in an automated system
4. Preparing written command security procedures
5. Preparing an emergency plan for the protection of classified materials
6. Reviewing and inspecting the effectiveness of the program in subordinate commands

Security Manager

Each command in the Navy and Marine Corps eligible to receive classified information is required to designate a security manager. The command makes this appointment in writing.

The security manager position may be assigned as a full-time, part-time, or collateral duty. The person designated is an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the command program. The security manager is a U.S. citizen and has a satisfactory background investigation (BI). The rank and grade requirements are firm. Designation of enlisted personnel or civilians below the grade of GS-11 is not allowed unless a waiver is granted. Waiver of the rank and grade requirements is rarely granted. Requests for waiver of the BI requirements, pending completion of the investigation, are usually granted.

Commands must designate and identify the security manager by name to all members of the command. The security manager's name should appear on organization charts, telephone listings, rosters, and so forth. Where the security manager appears on the organization chart depends on the command organization. In the shipboard organization recommended in the *Standard Organization and Regulations of the U.S. Navy,* the security manager is the executive officer's assistant. The security manager is responsible to the commanding officer on matters of security but reports to the executive officer for the administration of the Information and Personnel Security Program. A clear-cut organization is extremely important for a collateral duty security manager.

The effectiveness of command management of the program depends on the importance the commanding officer gives it. One area of concern in security management is security manager tenure. Without a formal training program for security managers, on-the-job training must suffice. For a security manager to develop a high degree of expertise takes time.

The security manager is the command's principal adviser on information and personnel security. The security manager is responsible for the management of the program. That doesn't necessarily mean the security manager personally handles all the security duties. Many commands are organized to assign like duties to the same person. The personnel officer may handle personnel security, the training officer may be responsible for security education sessions, and so forth. Those persons assigned security duties could be senior to the security manager. However, the security manager should know what is going on in all areas of security within the command. Having this knowledge helps the security manager ensure the various pieces of the security program fit together properly. It also helps the security manager make sure those in the command who have security duties are kept abreast of policy changes and procedures. In addition, the security manager needs to know what is going on to help solve security problems. The job may involve close supervision, minor direction, or a combination of both. However the command is organized, the security manager is the key in developing and administering the command's Information and Personnel Security Program.

Effective management of the program requires the security manager to perform the following functions:

- Serve as the commanding officer's adviser and direct representative in matters pertaining to the security of classified information and personnel security
- Develop written command information and personnel security procedures and integrate emergency destruction bills with the emergency plan
- Formulate and coordinate a command security education program
- Ensure threats to security, compromises, and other security violations are reported, recorded, and investigated
- Ensure incidents falling under the investigative jurisdiction of the Naval Investigative Service (NIS) are immediately referred to the nearest NIS office
- Administer the command program for classification, declassification, and downgrading of classified information
- Coordinate the preparation of classification guides in the command
- Maintain liaison with the command public affairs officer concerning security review of information proposed for public release
- Set accounting and control requirements for classified materials, including receipt, distribution, inventory, reproduction, and disposition
- Coordinate, with the security officer, physical security measures for protection of classified materials
- Ensure electrical or electronic processing equipment meets the requirements for control of compromising emanations
- Ensure security control of classified visits to and from the command
- Ensure protection of classified information during visits to the command when the visitor is not authorized access to classified information
- Prepare recommendations for the release of classified information to foreign governments
- Ensure classified contracts with Department of Defense (DOD) contractors comply with the Industrial Security Program
- Ensure all personnel who handle classified information or are assigned to sensitive duties are appropriately cleared
- Ensure requests for personnel security investigations are properly prepared, submitted, and monitored
- Ensure access to classified information is limited to those with the need to know
- Ensure all personnel security investigations, clearances, and access to classified information are recorded
- Coordinate the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties

- Maintain liaison with the command special security officer concerning investigations, access to sensitive compartmented information (SCI), continuous evaluation of eligibility, and changes to information and personnel security policies and procedures

- Maintain control of all foreign travel reported by assigned personnel

- Coordinate with the command automatic data processing (ADP) officer and physical security officer on areas of mutual concern

Top Secret Control Officer

Each command that handles Top Secret information designates, in writing, a Top Secret control officer (TSCO). The security manager may also be designated as the TSCO.

The person designated as TSCO is an officer; a chief petty officer; a senior noncommissioned officer (E-7, E-8, or E-9); or a civilian employee, GS-7 or above. The TSCO is a U.S. citizen with a final Top Secret clearance. Only a reliable person of mature judgment is chosen as TSCO. The TSCO should be completely familiar with the requirements for protection of Top Secret information.

The TSCO is responsible to the security manager (if not the same person) for Top Secret materials in the command. This responsibility includes the receipt, custody, accounting for, and disposition of Top Secret materials.

The TSCO performs the following duties:

- Maintains a system of accountability for all Top Secret materials in the command. Records the source, downgrading, movement from one office to another, current custodian, and destruction or other disposition of the Top Secret materials.

- Keeps dissemination of Top Secret information to the absolute minimum necessary for proper planning or action. No "standatd routing" of Top Secret materials is allowed in a command.

- Transmits Top Secret materials within the command by direct personal contact. The TSCO doesn't have to deliver the materials personally, but the materials should be delivered directly to the person who will assume responsibility for them. Top Secret materials should never be dropped in an "in" basket.

- Maintains a continuous collection of signed receipts and disclosure records for all Top Secret materials. Person-to-person contact is mandatory for the receipting.

- Ensures physical inventories of Top Secret materials are conducted at least once annually.

- Maintains a current roster of persons within the command who are authorized access to Top Secret information. The TSCO should know who requires access and be able to assist the security manager in determining access granted by the command.

- Ensures all Top Secret materials are accounted for and properly transferred when custodians are relieved of their duties. This requirement applies to the subcustodians of the command as well as the TSCO.

Security Assistants

Large commands often assign assistant security managers or departmental security coordinators. Too often, command security managers assume that by designating different levels of security managers in the command, they have discharged their responsibilities. Inspections of major commands have shown that the security manager of an element within a command is usually doing little more than classified material control. The size or complexity of the command may demand delegation. In such cases, command security managers should realize they are still responsible for the command's Information and Personnel Security Program as a whole. The command security manager should provide the guidance, coordination, and direction necessary to ensure all of the program is being administered effectively.

The assistant security manager is a U.S. citizen; an officer or an enlisted person, E-6 or above; or a civilian employee, GS-6 or above. The assistant security manager is designated in writing. The assistant security manager needs a background investigation only when authorized to issue security clearances (that is, sign the clearance

CERTIFICATE OF PERSONNEL SECURITY INVESTIGATION, CLEARANCE AND ACCESS

OPNAV 5520/20 (Rev. 10-79) S/N 0107-LF-055-2101 *(For Use, See OPNAVINST 5510.1)*

PLEASE TYPE

PART I – IDENTIFICATION DATA

Name	Date of Birth	Place of Birth	SSN
CHRISTMAS, MARY (N)	570415	PLYMOUTH, ENGLAND	333-33-333

Status: ☐ OFFICER ☒ ENLISTED ☐ CIVILIAN

Grade	Service	Service Date
YN1	USN	760510

Citizenship Verified

☐ U.S. NATIVE

☒ U.S. NATURALIZED 750303/9246543 *(Certificate Number)*

☐ IMMIGRANT ALIEN *(See Comments)* _____ *Registration Number*

☐ PHILIPPINE NONIMMIGRANT ALIEN *(See Comments)*

PART II – RECORD OF INVESTIGATION

TYPE	AGENCY	DATE	CASE CONTROL NO.	TYPE	AGENCY	DATE	CASE CONTROL NO.
ENTNAC	DIS	760612	N/A	SBI-PR	DIS	870817	871671330
BI	DIS	771018	772281452				
NAC	DIS	830228	N/A				
SBI	DIS	830709	831232175				

PART III – RECORD OF CLEARANCE

DATE	CLEARANCE *(Indicate Interim or Final)*	BASIS/DATE	CERTIFYING COMMAND *(Signature, Typed Name and Command)*	REMARKS
760620	Final Secret	ENTNAC/760612	J. A. Doe J. A. DOE XO SSC SAN DIEGO	
770724	Interim Top Secret	ENTNAC/760612	J. R. Frost J. R. FROST CO USS ARGO	BI Req 770724 Exp 780124
771030	Final Top Secret REVOKED	BI/771018	J. R. Frost J. R. FROST CO USS ARGO	See Comments
790328	Final Top Secret	BI/771018	J. R. Frost J. R. FROST CO USS ARGO	See Comments
830715	Final Top Secret	SBI/830709	W. T. Door W. T. DOOR XO USS SUNFISH	
870822	Final Top Secret	SBI PR/870817	P. T. Boat P. T. BOAT XO FICLANT	

SAMPLE

DATE:	COMMENTS
910206	Clearance revoked per CO USS ARGO ltr ser 121 of 6 Feb 1991
910328	Clearance reinstated per COMNAVMILPERSCOM ltr NMPC-81/103 of 15 Mar 1991
910315	Satisfactory NAC completed 830228 for PRP Controlled billet

W. T. Door
W. T. DOOR
XO USS SUNFISH

Copy to: *(Mil. Pers. only)* NAVY – Commander, Naval Military Personnel Command (NMPC 81) | MARINE CORPS – Commandant of the Marine Corps (MSRB)

Figure 9-l.-Sample 0PNAV Form 5520/20.

entry on the OPNAV Form 5520/20). Figure 9-1 shows a sample OPNAV Form 5520/20. Otherwise, the investigative and clearance requirements depend on the level of access to classified information needed.

Security clerks may be assigned without regard to rate or grade as long as they have the clearance needed for the access they will have.

Top Secret control assistants (TSCA) maybe assigned as needed and are designated in writing. The TSCA is a U.S. citizen, E-5 or above, or a civilian employee, GS-5 or above who has a final Top Secret clearance. TSCAs maybe authorized to take the following actions:

Sign courier receipts and transfer of custody receipts for Top Secret materials

Certify materials being transferred into Defense Courier Service and sign on behalf of the Top Secret control officer

Transmit Top Secret materials

Conduct required page checks of Top Secret documents

Top Secret couriers, or others who handle Top Secret materials, are not considered to be TSCAs. They must have a Top Secret clearance, an understanding of the importance of the materials, and familiarity with the procedures for handling Top Secret materials. No grade or rate restrictions apply to Top Secret couriers.

AUTOMATED DATA PROCESSING (ADP) SECURITY OFFICER.—Each command involved in processing data in an automated system designates an ADP security officer.

The ADP security officer is responsible to the security manager for the protection of classified information being processed in the automated system. The ADP security officer is responsible to the physical security officer for the protection of personnel, equipment, and related resources.

SPECIAL SECURITY OFFICER. —Certain commands in the Department of the Navy are accredited for and authorized to receive, process, and store sensitive compartmented information (SCI). These commands have a designated sensitive compartmented information facility (SCIF). A special security officer (SSO) is responsible for the operation of that SCIF and the security, control, and use of SCI. The SS0 is an officer or a civilian employee, GS-9 or above. All matters relating to SCI or SSO requirements are referred to SSO.

For additional information on commands authorized to receive, process, and store SCI materials, consult OPNAVINST 5510.lH.

Security Education

Each command that handles classified information establishes and maintains an active security education program to instruct all personnel in security policies and procedures.

Commands need a security education program to teach the proper way to protect classified information from hostile threats. The purpose of this program is to ensure we understand the need to protect classified information and know how to safeguard it. The goal is to develop fundamental habits of security to the point that we automatically exercise proper discretion. Once we develop the proper habits, the security of classified information becomes a natural element of every task.

COMNAVSECINVCOM (OP-09N) is responsible for policy guidance, education requirements, and source support for the security education program. The development of security education materials for use in the Navy or Marine Corps should be coordinated with OP-09N. You do not have to coordinate development with OP-09N if you are preparing the materials for use in your command program. OP-09N reviews any curriculum material being prepared for a formal training environment to make sure current policies and procedures are being taught.

Training commands indoctrinate personnel entering the Navy and Marine Corps about classified information. They indoctrinate new members to ensure they have a basic understanding of what is meant by classified information and why and how it is protected. Civilians being employed by the Department of Defense for the first time also receive this basic indoctrination.

The security manager is responsible to the commanding officer for security education. As a supervisor you must identify the security requirements for your work center functions. Once you do that, ensure your personnel are familiar with those requirements. Make on-the-job training an essential part of command security education.

Provide security education to all personnel, whether they have access to classified information or not. Provide more extensive education for

those who do have access. Tailor your education efforts to meet the needs of the command.

In developing your command security education program, provide the minimum briefing requirements. Make sure the program does not evolve into a system of meeting formal requirements without achieving the real goals. For instance, giving the same lecture or showing the same film every year would satisfy the requirement for an annual refresher briefing. However, it would not enhance security awareness.

The objective of the overall program is to advise personnel of the following facts about security:

1. The adverse effects to the national security that could result from unauthorized disclosure of classified information; their personal, moral, and legal obligation to protect classified information within their knowledge, possession, or control
2. Their responsibility to adhere to those standards of conduct required by persons holding positions of trust and to avoid personal behavior that could render them ineligible for access to classified information or assignment to sensitive duties
3. Their obligation to notify their supervisor or command security manager of a potentially serious security violation by someone who has access to classified information or is assigned to sensitive duties
4. The requirement of supervisors to continuously evaluate the eligibility of personnel for access to classified information or assignment to sensitive duties
5. The principles, criteria, and procedures for classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and materials; the strict prohibitions against the improper use and abuse of the classified system
6. The procedures for challenging classification decisions they believe to be improper
7. The security requirements of their particular assignments
8. How to determine, before disseminating classified information, that the prospective recipient has been authorized access by competent authority, needs the information to perform his or her official duties, and can properly protect (store) the information
9. The strict prohibition against discussing classified information over an unsecured telephone or in any manner that may permit interception by unauthorized persons
10. The techniques employed by foreign intelligence activities in attempting to obtain classified information
11. The penalties for engaging in espionage activities and for mishandling classified information or materials
12. Their obligation to report counterintelligence activities as outlined in chapter 5 of OPNAVINST 5510.1H

BASIC SECURITY EDUCATION. —All persons attend basic security education indoctrination or orientation classes after their initial entry into the service. The indoctrination classes are designed to give every person in the Navy a basic understanding of classified materials and how and why this information should be protected. Orientation training is designed for those persons who will have access to classified material, The following guidelines are the minimum requirements for basic security education:

1. Indoctrination in basic principles of security upon entering the Navy
2. Orientation of those persons who will have access to classified information at the time of their duty assignment
3. On-the-job training in specific requirements for the duties assigned
4. Annual refresher briefings for those who have access to classified information
5. Special briefings as circumstances dictate
6. Debriefing each time a security termination statement is executed
7. Counterespionage briefings once every 2 years for those who have access to information classified Secret or above

When you indoctrinate personnel, teach them to take the following security precautions:

1. Protect information essential to the national security from disclosure to unauthorized persons
2. Mark all classified materials to show the level of classification
3. Allow access to classified information only to officially and specifically authorized persons

4. Store and use classified material only in secure areas, protect it during transfer from one area (or command) to another, and destroy it only by authorized means
5. Report any breach of security
6. Report any contact with citizens of Communist-controlled or hostile countries
7. Report any attempt by an unauthorized person to solicit classified information

Make sure each person who will have access to classified information receives orientation and signs a nondisclosure agreement. Provide the orientation and have the person sign the statement as soon as possible after reporting aboard or before their assignment to duties involving access to classified information.

The timing and format for orientation will vary, depending on the size of the command. However, having persons certify that they have "read and understand" the provisions of security matters is not adequate orientation. Describe the command security organization and identify the security manager by name. Give personnel enough information to make them realize they are an essential link in the security structure of the command. Make sure you tell new members about any special security precautions for your command. For instance, if your command has foreign national students or personnel in exchange programs, alert new members to the restrictions on access by foreign nationals. If your command has a coded badge system, explain the significance of the different codes.

The security orientation should fit the command and the person receiving it. Place more emphasis on security procedures when a new member has not had previous experience with handling classified information.

CONTINUING SECURITY EDUCATION.— Once personnel have received the basic security education training, make sure they take part in a continuing security education training program. Guarding against security compromises and other violations is vital to our nation's security. The various programs that protect our security include on-the-job training, refresher and special briefings, and debriefings.

On-The-Job Training. —Your personnel need to know the security procedures required for the duties they perform. On-the-job training is the phase of security education in which personnel learn to apply specific security procedures.

Compromised reports often show that breaches of security are caused by supervisors who assume subordinates know what they are supposed to do. Examples include assigning people to mail rooms without training them in the preparation and transmission of classified material or designating a Top Secret control officer without reviewing control requirements. Allowing subordinates to learn by the trial-and-error method risks security as much as assuming they know how to protect classified information.

Refresher Briefings. —Once a year, make sure all personnel who have access to classified information receive a refresher briefing. The refresher briefing should enhance security awareness—it should not rehash the basics or be a repeat of the same program year after year.

Once every 2 years, an NIS agent should give a counterespionage briefing to those persons who have access to materials classified as Secret or above. The security manager is responsible for arranging the briefing with the local NIS office.

Arrange for various types of special briefings as needed. They could include briefings on foreign travel, the North Atlantic Treaty Organization (NATO), and single integrated operational plan-extremely sensitive information and sensitive compartmented information.

Debriefings. —Persons who have had access to classified information should receive a debriefing at the following times:

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

2. At the conclusion of an access period, when a Limited Access Authorization has been granted

3. When the person's security clearance is revoked for cause

4. When a person's security clearance is administratively withdrawn

SECURITY TERMINATION STATEMENT

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

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

Chief of Naval Operations

(Op-09B21)

Washington, DC 20350

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

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

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

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

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

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

SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE *(Fill in first, middle, and last name. If military, indicate rank or rate. If civilian indicate grade.)*
Jon T. Boate	Mary (N) Christmas
TYPE OR PRINT NAME OF WITNESS JON T. BOATE	DATE 841018

S-14581

Figure 9-2.-Security Termination Statement.

Members are also debriefed and required to sign a Security Termination Statement (fig. 9-2) if they inadvertently gain access to information they aren't qualified to receive.

The debriefing should clearly stress the following security precautions:

1. Personnel are to return all classified materials in their possession.
2. Personnel are no longer eligible for access to classified information.
3. Personnel may never divulge classified information; orally or in writing, to any unauthorized person or in judicial, quasi-judicial, or administrative proceedings without first receiving written permission from OP-09N.
4. Personnel may receive severe penalties for disclosure.
5. Personnel are to report to NIS any attempt by an unauthorized person to solicit classified information. (Any attempts are reported to the FBI or nearest DOD component if personnel are no longer affiliated with the Department of the Navy.)

When a clearance is being revoked, a person occasionally may refuse to sign the Security Termination Statement during the debriefing. If that happens, stress that the refusal to sign doesn't change the person's obligation to protect classified information from unauthorized disclosure. Send a copy of the termination statement, which shows that the person refused to sign the statement, to OP-09.

COMPROMISE AND OTHER SECURITY VIOLATIONS

Two types of security violations occur. One involves the compromise or possible compromise of classified information. The other involves a violation of security regulations, but does not involve a compromise.

Compromise is the disclosure of classified information to a person who is not authorized access to that information. The unauthorized disclosure may have occurred knowingly, willfully, or through negligence. Conclusive evidence that classified information has been disclosed to an unauthorized person confirms the existence of a compromise.

Discovery of Compromise

If you discover a compromise of classified material, you should regain custody of the material, if possible, and give it the proper protection. Then notify NIS, who may begin an investigation independent of command inquiries.

PRELIMINARY INQUIRY. —A preliminary inquiry will be conducted when classified information has been compromised or subjected to compromise. The inquiry should be completed quickly, usually within 2 or 3 days.

Every effort should be made to keep the inquiry Unclassified. The occurrence of a compromise does not necessarily require a classified inquiry.

The inquiry may reveal that the compromise presents a minimal risk. If you find no significant command security weaknesses, you do not have to take formal disciplinary action. In such cases, send the report of preliminary inquiry, by endorsement, to the next senior in the administrative chain and who has Top Secret classification authority.

JUDGE ADVOCATE GENERAL (JAG) MANUAL INVESTIGATION. —A *JAG Manual* investigation is an administrative investigation based on chapters II through VI of the *Manual of the Judge Advocate General.* The command having custodial responsibility for the material compromised convenes the investigation. The purpose of a *JAG Manual* investigation is to answer, in detail, questions about the *who, what, where, when,* and *why* of the security violation. The *JAG Manual* investigation gives the command an opportunity to make a critical review of its security posture.

Other Security Violations

The commanding officer may act without reporting to higher authority on a violation of a security regulation not resulting in compromise or subjection to compromise. However, the commanding officer must ensure that type of security violation is investigated just as thoroughly as one resulting in a compromise because it shows a weakness within the security program. Commanding officers may decide if the occurrence of that security violation justifies some form of corrective action. The possibility of persons receiving disciplinary action for that type of violation is just as great as it is for a violation

SECURITY DISCREPANCY NOTICE
OPNAV 5511/51 (3-80) S/N 0107-LF-055-5355 (This form replaces OPNAV 5511/8; 22 and 24 which are obsolete)

FROM	DATE
Chief of Naval Operations, Washington, DC 20350	16 Aug 1989

REF a. Your ltr ser S53 of 18 Aug 1983 (Insert ref. (a)) b. OPNAVINST 5510.1 SERIES

ENCL

SAMPLE

TO:
Commanding Officer
USS NEVERSAIL
FPO San Francisco 94035

(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

X	SENT VIA NON-REGISTERED/ NON-CERTIFIED MAIL		CLASSIFICATION NOT MARKED ON INNER CONTAINER		RECEIVED IN POOR CONDITION; COMPROMISE IMPROBABLE
X	SENT IN SINGLE CONTAINER	X	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: OP-009D (WITH ADDRESSEE DELETED)

SIGNATURE	TITLE
Jack R. Frost	Security Manager, Op-009P

Figure 9-3.-Security Discrepancy Notice, OPNAV Form 5511/51.

leading to compromise. Those responsible for security violations may be reevaluated to determine if they should remain eligible for access to classified information.

If you find assigned personnel have left unattended and unlocked a container in which classified material is stored, report the incident immediately to the senior duty officer. The container will be guarded until the duty officer arrives at the location of the unlocked container. The duty officer will then inspect the classified material involved, lock the container, and make a security violation report to the commanding officer. If a possibility of compromise exists, the person responsible for the container is required to return to the ship or station to make a complete inventory of its contents.

When you receive classified material that shows improper handling, but no compromise has occurred, promptly notify the commanding officer of the sending activity. Improper handling of classified material, such as improper mailing, shipping, wrapping, addressing, packaging, or transmitting, can result in security discrepancies. The following are other security discrepancies that can result from improper handling:

- Sending classified information in single containers
- Failing to enclose a return receipt for Secret material
- Sending Confidential information by First Class instead of Registered mail to FPO/APO addresses
- Failing to mark the classification on the inner container

Report such violations on a Security Discrepancy Notice, OPNAV Form 5511/51 (fig. 9-3).

Classified material that enters a foreign postal system because of improper addressing or other mishandling is considered to have been compromised. Similarly, when containers of classified information are damaged in shipment to the extent that the contents are exposed, the possibility of compromise again exists. Both of these two situations require a preliminary inquiry and a *JAG Manual* investigation.

COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO THE NAVAL INVESTIGATIVE SERVICE

Certain matters affecting national security must be reported to the NIS so that appropriate counterintelligence action can be taken. All Department of the Navy employees, military and civilian, should report to their commanding officers or to the nearest command any suspicious activities. Suspicious activities include possible acts of sabotage, espionage, or compromise or contact with citizens of hostile countries. Personnel should report such activities if they involve themselves, their dependents, or others, whether or not they have access to classified information. Commanding officers should, in turn, notify the nearest Naval Investigative Service office immediately.

Sabotage, Espionage, or Deliberate Compromise

Report all available information about possible acts of sabotage, espionage, deliberate compromise, or other subversive activities to your commanding officer. If you are away from your command, report such activities to the most readily available command. Your commanding officer or the command to which you report the activity will, in turn, notify the nearest NIS office. If you cannot immediately contact NIS when sabotage, espionage, or a person's immediate flight or defection threatens security, notify COMNAVSECINVCOM by classified IMMEDIATE message. List the CNO as an information addressee.

Notify the servicing NIS office immediately of any requests, through other than official channels, for classified defense information, Report anyone who makes such requests, regardless of nationality. Report any requests for information from any person believed to be in contact with a foreign intelligence service. Also report requests for information such as the following:

- Names, duties, personal data, and characterizations of Department of the Navy personnel
- Technical orders, manuals, regulations, base directories, personnel rosters; and unit manning tables
- The designation, strength, mission, combat posture, and development of ships, aircraft, and weapons systems

NIS will advise you of any further action to take and will coordinate other actions with members of the U.S. intelligence community. In remote locations where you cannot contact NIS quickly enough, you may contact field representatives of other U.S. intelligence agencies.

Contacts With Citizens of Hostile Countries

Report to NIS any form of contact, intentional or otherwise, with any citizen of a Communist-controlled country or country hostile to the United States. The term *contact* means any form of encounter, association, or communication with any citizen of a Communist-controlled or hostile country. That includes cent acts in person or by radio, telephone, letter, or other forms of communication for social, official, private, or any other reasons. Report to NIS any visits you make to embassies, consulates, trade or press offices, or other official establishments of these countries.

Contacts and other associations with citizens of Communist-controlled or hostile countries are not, in themselves, wrong, against regulations, or illegal. However, report the contact immediately so that NIS may evaluate the contacts to protect the Department of the Navy from hostile intelligence activities. This policy applies to all Department of the Navy personnel, military and civilian, including active-duty Reserve personnel.

Suicide or Attempted Suicide

If a Department of the Navy member who had access to classified information commits suicide or attempts suicide, the commanding officer immediately reports the incident to the nearest NIS office. The commanding officer forwards all available information about the incident by the quickest means possible. COMNAVSECINVCOM receives an information copy of the report. The report explains the nature and extent of the classified information to which the individual had access.

The NIS office receiving the report coordinates the investigation with the commanding officer. If NIS assumes immediate investigative responsibility, command investigative efforts are subordinate to those of the NIS.

Unauthorized Absence

When a Department of the Navy member who had access to classified information is in an unauthorized absence status, the commanding officer conducts an inquiry. The purpose of the inquiry is to determine if the member's activities, behavior, or associations may be detrimental to the interest of national security. If such indications exist, the commanding officer reports all available information by the quickest means to the nearest NIS office. COMNAVSECINVCOM also receives a report of the information.

Foreign Travel

Persons with a security clearance should report to their security office before performing any foreign travel. Failure to report trips abroad or frequent foreign travel should be investigated. Any unusual circumstances involving foreign travel should be referred to the nearest NIS office and to COMNAVSECINVVOM.

CLASSIFIED MATERIAL

Classified material is any product containing information that could adversely affect the national security if disclosed without authorization. Although the Department of the Navy must prevent the release of classified material to the public, it releases as much information about its activities as possible. Therefore, commands only assign security classifications to information as needed to protect national security.

When assigning security classifications, avoid classifying information unnecessarily or giving it a higher than necessary classification. If you have reasonable doubt about the need to classify information, safeguard it as if it were classified at least Confidential. You may then request that the original classification authority (OCA) determine if the classification should be changed. The same logic applies to the appropriate level of classification. Safeguard the information as if it were classified at the higher level until the OCA can make a determination. The OCA should make a determination within 30 days.

CLASSIFICATION DESIGNATIONS

Information that requires protection against unauthorized disclosure in the interest of national security receives one of three classification designations: Top Secret, Secret, or Confidential. Do not use the markings For Official Use Only and Limited Official Use to identify classified information. Neither use modifying terms, such

as *sensitive,* in conjunction with authorized classification designations.

Designate a Top Secret classification to information that could cause grave damage to our national security upon unauthorized disclosure, such as the following:

- Armed hostilities against the United States or its allies
- Disruption of foreign relations vitally affecting the national security
- Compromise of vital national defense plans or complex cryptologic and communications intelligence systems
- Disclosure of sensitive intelligence operations
- Disclosure of scientific or technological developments vital to national security

Designate a Secret classification to information that could cause serious damage to the national security upon unauthorized disclosure, such as the following:

- Disruption of foreign relations significantly affecting national security
- Significant impairment of a program or policy directly related to the national security
- Disclosure of significant military plans or intelligence operations
- Compromise of significant scientific or technological developments relating to national security

Designate a Confidential classification to information that could cause damage to our national security upon unauthorized disclosure, such as the following:

- Information indicating strength of ground, air, and naval forces
- Performance characteristics, test data, design, and production data on U.S. weapons systems and munitions

DECLASSIFICATION AND DOWNGRADING AUTHORITY

The following officials are authorized to declassify and downgrade information:

1. The Secretary of the Navy with respect to all information over which the Department of the Navy exercises final classification authority
2. The original classification authority as designated by the Secretary of the Navy, a successor to the original classification authority, or a supervisor of either
3. The Deputies or Chiefs of Staff to those original classification authorities for classified information in their functional areas

Only the Secretary of Defense or the Secretary of the Navy may decide that specific information no longer requires the protection originally assigned. That is, they may change the original classification, which will change the classification guidance for that information. Do not confuse the authority to downgrade or declassify with the authority for administrative responsibility. The person who has administrative responsibility may downgrade or declassify information as directed by a classification guide, the continued protection guidelines, or the declassification instructions on a document.

Systematic Declassification Review

As classified (permanently valuable) records in the National Archives become 30 years old, the Archivist of the United States reviews them for declassification.

The CNO, OP-09N, specifies which 30-year old Department of the Navy information requires continued protection. In coordination with Navy and Marine Corps commands, OP-09N has developed continued protection guidelines for the Archivist. The Director, Naval Historical Center, designates experienced personnel to guide and help the Archivist. These personnel guide and assist National Archives employees in identifying and separating documents that require continued classification. The Director, Naval Historical Center, refers doubtful cases to the command having original classification jurisdiction.

The CNO, OP-09N, reviews the continued protection guidelines at least every 5 years. This review identifies additional information becoming

30 years old that requires continued protection and confirms the continued need for classification of previously identified information.

Certain categories of information transferred to the National Archives are exempted from 30-year systematic review; instead, the Archivist reviews the information when it becomes 50 years old. These categories consist of intelligence (including special activities), intelligence sources or methods created after 1945, and cryptology created after 1945. The Archivist reviews restricted data and formerly restricted data upon request. Foreign government information is declassified only if specified or agreed to by the foreign entity.

Special procedures developed by the Director, National Security Agency, in consultation with affected agencies, govern the systematic review and declassification of classified cryptologic information. The Secretary of Defense must approve the procedures.

Mandatory Declassification Review

A United States citizen or immigrant alien, a federal agency, or a state or local government may request a review for declassification of Department of the Navy information. Information originated by the following people are exempt from these provisions for mandatory review for declassification:

- The President
- The White House Staff
- Committees, commissions, or boards appointed by the President
- Others specifically providing advice and counsel to the President

UPGRADING

Original classification authorities may upgrade classified information, within their functional areas of interest, only under the following conditions:

1. When all known holders of the information can be promptly notified
2. When all known holders of the information are authorized access to the higher level of classification or the information can be retrieved from the known holders not authorized access to the higher level of classification

Original classification authorities may classify information previously determined to be Unclassified only under the following conditions:

1. When all known holders of the information can be promptly notified
2. When all known holders of the information are authorized access to the higher level of classification or the information can be retrieved from the known holders not authorized access to the higher level of classification
3. When control of the information has not been lost
4. When loss of control can still be prevented

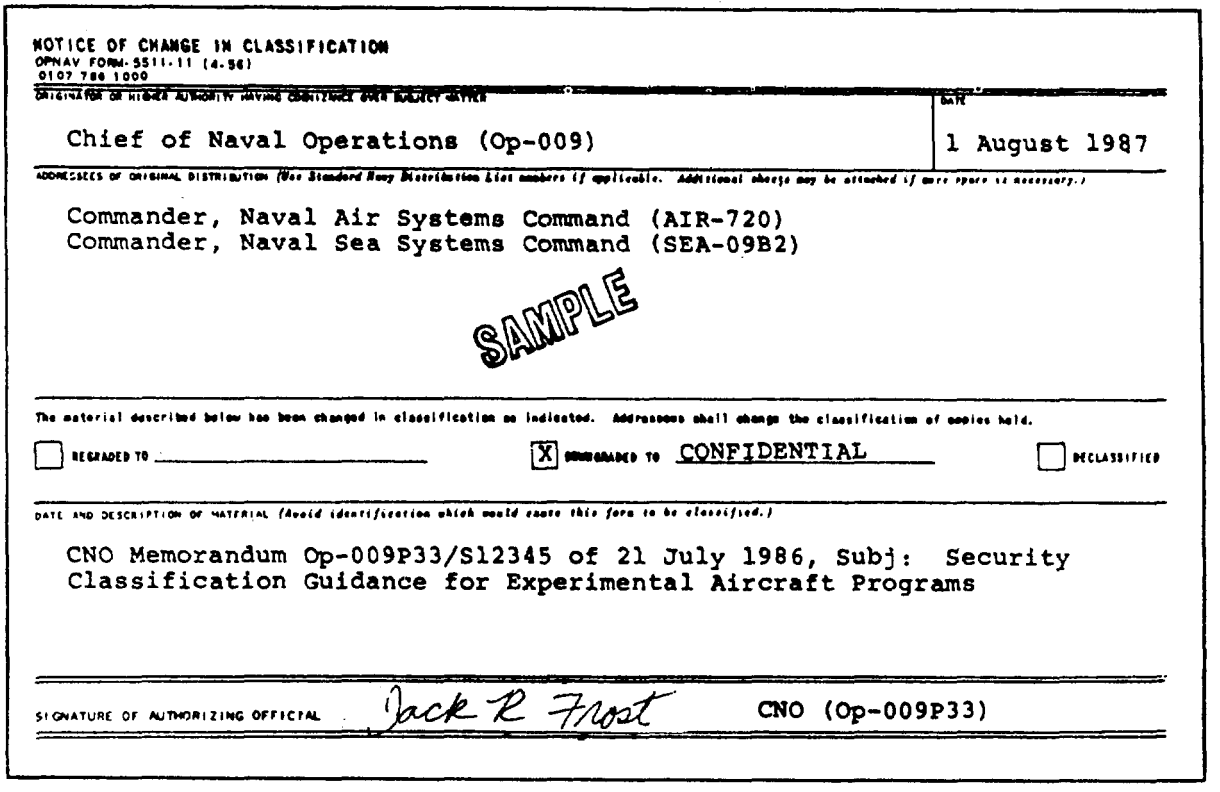
Make every effort to retrieve, safeguard, and properly mark and control properly classified information that has been underclassified or disseminated as Unclassified.

Notices are not issued to downgrade or declassify materials that contain instructions for downgrading or declassification. All original addressees will be notified of changes that shorten or lengthen the duration of classification of the material or that change the classification level. A notice assigning classification to currently Unclassified information will be classified Confidential, unless the notice itself contains information at a higher level. You may use OPNAV Form 5511-11 (fig. 9-4) for that purpose.

REPRODUCTION OF CLASSIFIED MATERIAL

Because so many reproduction machines are used throughout the Navy, the problems associated with reproducing classified material have continued to grow. Therefore, commanding officers control the number of copies of classified documents reproduced within their commands. Personnel must have proper authorization to reproduce classified material on reproduction machines. The originating activity or higher authority must consent to the reproduction of Top Secret information.

Commanding officers designate certain officials to approve all requests to reproduce Top Secret and Secret materials. These officials, in turn, ensure that security procedures for the reproduction of classified materials are followed and that such reproduction is kept to a minimum. Make certain your personnel are aware of the requirement for approval by one of these designated officials before reproducing classified material.



NOTICE OF CHANGE IN CLASSIFICATION
OPNAV FORM 5511-11 (4-86)
0107 780 1000

ORIGINATOR OR HIGHER AUTHORITY HAVING CognIZANCE OVER SUBJECT MATTER | DATE

Chief of Naval Operations (Op-009) | 1 August 1987

ADDRESSEES OF ORIGINAL DISTRIBUTION (Use Standard Navy Distribution List numbers if applicable. Additional sheets may be attached if more space is necessary.)

Commander, Naval Air Systems Command (AIR-720)
Commander, Naval Sea Systems Command (SEA-09B2)

SAMPLE

The material described below has been changed in classification as indicated. Addressees shall change the classification of copies held.

☐ REGRADED TO _____ ☒ DOWNGRADED TO CONFIDENTIAL ☐ DECLASSIFIED

DATE AND DESCRIPTION OF MATERIAL (Avoid identification which would cause this form to be classified.)

CNO Memorandum Op-009P33/S12345 of 21 July 1986, Subj: Security Classification Guidance for Experimental Aircraft Programs

SIGNATURE OF AUTHORIZING OFFICIAL Jack R Frost CNO (Op-009P33)

Figure 9-4.-Notice of Change in Classification, OPNAV Form 5511-11.

Where possible, two people will be involved in reproducing classified material to ensure the positive control and safeguard of reproduced material.

Commands maintain records for 2 years to show the number and distribution of all reproductions of classified documents, including the following:

Top Secret documents

Classified documents covered by special access programs distributed outside the originating agency

Secret and Confidential documents marked with special dissemination and reproduction limitations

Your command should designate specific areas and equipment for there production ofclassified material. Prominently display signs on or near the equipment to advise users of the designation. For example, a sign may read, THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY (designated official). If you have machines that are not authorized for the reproduction of classified material, post a warning notice, such as the following, on the machine: THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL. Make sure a designated official can easily see the area to ensure the authorization of copies and reproduction of the minimum number of copies.

Some equipment may use extremely sensitive reproduction paper. Use and store the paper in a manner to prevent image transfer of classified information.

When reproducing material, make sure it shows the classification and other special markings that appear on the original material. Double check all reproduced material, and remark reproduced copies that have unclear markings.

Safeguard all samples, waste, or overruns resulting from the reproduction process according to the classification of the information involved. Destroy the materials promptly as classified waste. Check areas surrounding reproduction equipment for classified materials that may have been left on nearby desks or thrown in wastebaskets. If the

machine malfunctions, check to see that all copies have been removed. After reproducing classified materials, make sure the original and all copies have been removed from the machine.

SAFEGUARDING OF CLASSIFIED MATERIAL

Classified information or material is used only where facilities or conditions are adequate to prevent unauthorized persons from gaining access to it. The exact nature of security requirements depends on a thorough security evaluation of local conditions and circumstances. Chapter 13 of OPNAVINST 5510.1H contains specific details for safeguarding classified material.

Responsibility for Safeguarding

If you have possession of classified material, safeguard it at all times. Lock it in appropriate security equipment whenever the material is not in use. Follow procedures that ensure unauthorized persons cannot gain access to the classified information by sight, sound, or other means. Never discuss classified information with or in the presence of unauthorized persons.

When working with Top Secret information, observe the two-person rule. That rule requires two persons to handle Top Secret material. However, the rule allows one person to be left alone with the material for a short period of time during normal working hours.

Remove classified material from a designated office or working area ONLY in the performance of your official duties. Remove classified material from designated areas to work on it during off-duty hours, or for any other purpose, ONLY with specific approval of the Chief of Naval Operations (OP-09N) or appropriate authority. You will

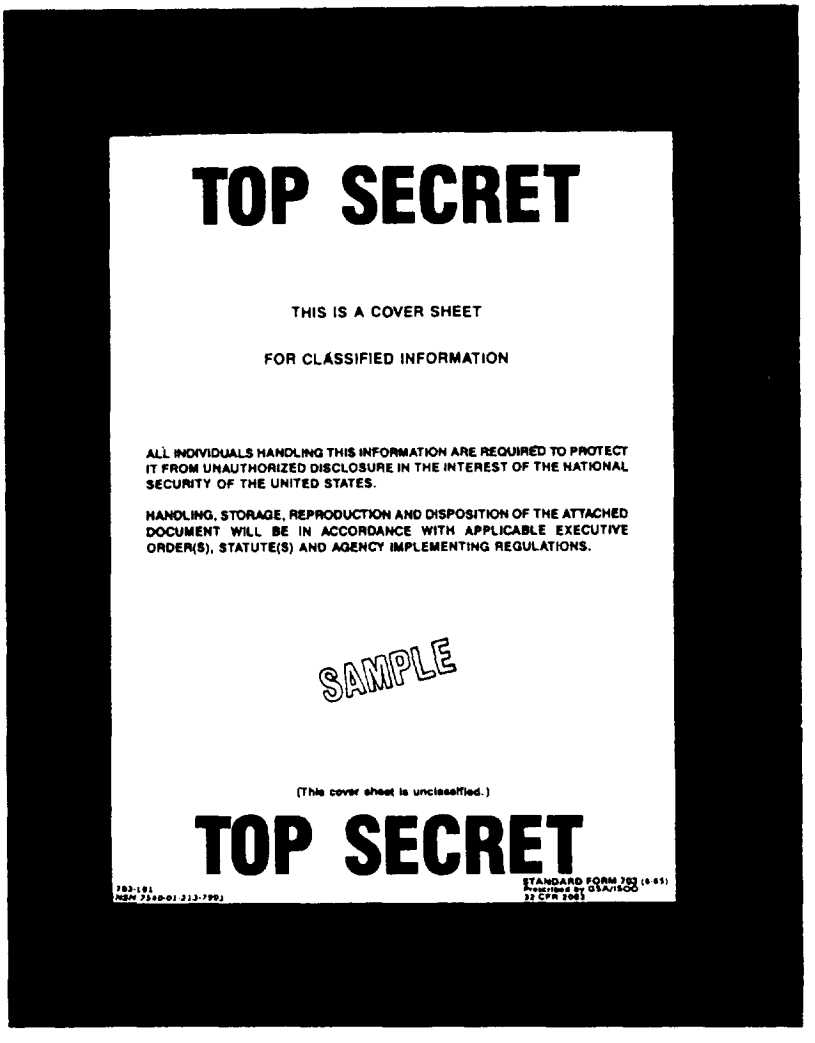


Figure 9-5.-Classified material cover sheet, Standard Form 703.

receive approval only when an overriding need occurs and you can provide the required physical safeguards, including *approved* storage. Your command must keep a list of the materials removed. You will receive approval for the removal of classified material overnight only when you have access to a secure government or cleared industrial facility for storage.

Restricted Areas

Different areas within a command may have varying degrees of security importance depending on the purpose and nature of the work, information, and materials concerned. In some cases, the entire area of a command may have a uniform degree of security importance. In others, differences in degree of security importance will require further segregation of certain activities. In locations where a language other than English is prevalent, display Restricted Area warning notices in English and the local language.

Do not designate controlled areas, limited areas, and exclusion areas in any way that outwardly notes their relative sensitivity. Identify any such area only as a "Restricted Area."

Care During Working Hours

During working hours, take the following precautions to prevent access to classified information by unauthorized persons:

- After removing classified documents from storage, keep them under constant surveillance and face down or covered when not in use. Classified material cover sheets, shown in figures 9-5, 9-6, and 9-7, are the only forms authorized for covering classified documents.

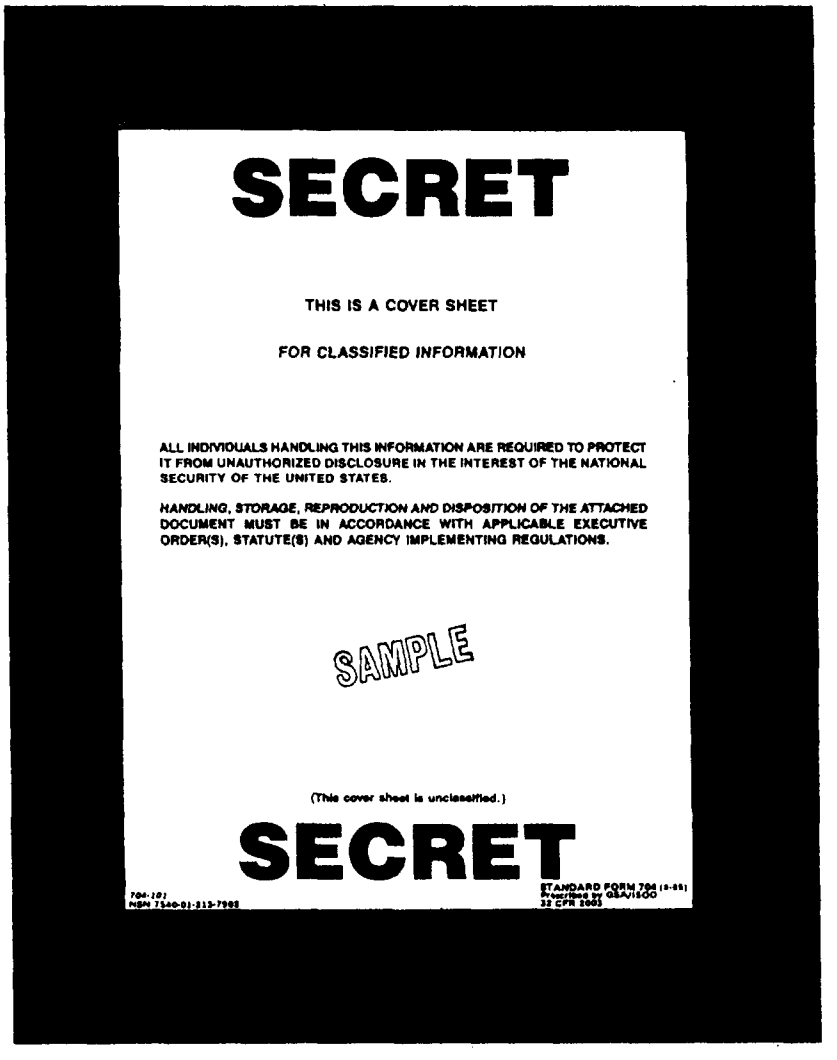


Figure 9-6.-Classified material cover sheet, Standard Form 704.

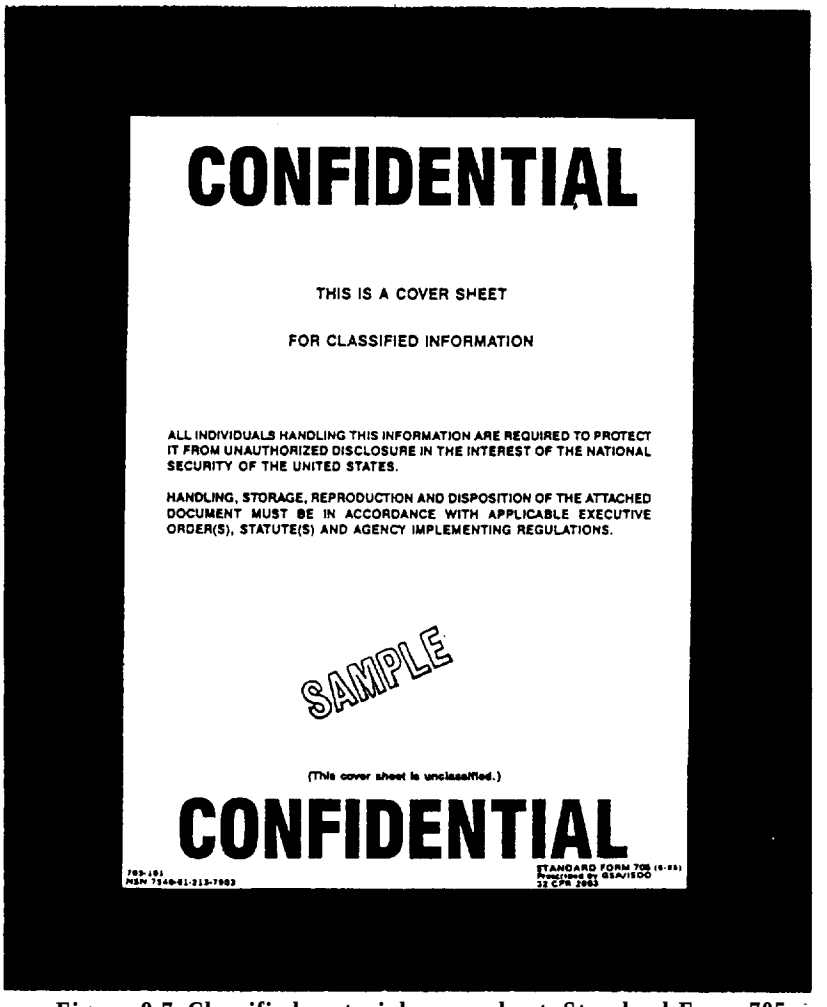


Figure 9-7.-Classified material cover sheet, Standard Form 705.

- Discuss classified information only if unauthorized persons cannot overhear the discussion. Take particular care and alert fellow workers when visitors, repair persons, or maintenance workers are present.

- Protect preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information. Either destroy them using an approved method or give them the same classification and safeguarding as the original classified material held.

- Protect typewriter ribbons used in typing classified material the same as for the highest level of classification for which they have been used. Also, destroy them as classified waste. Typewriter ribbons are exempt from destruction under the following conditions:

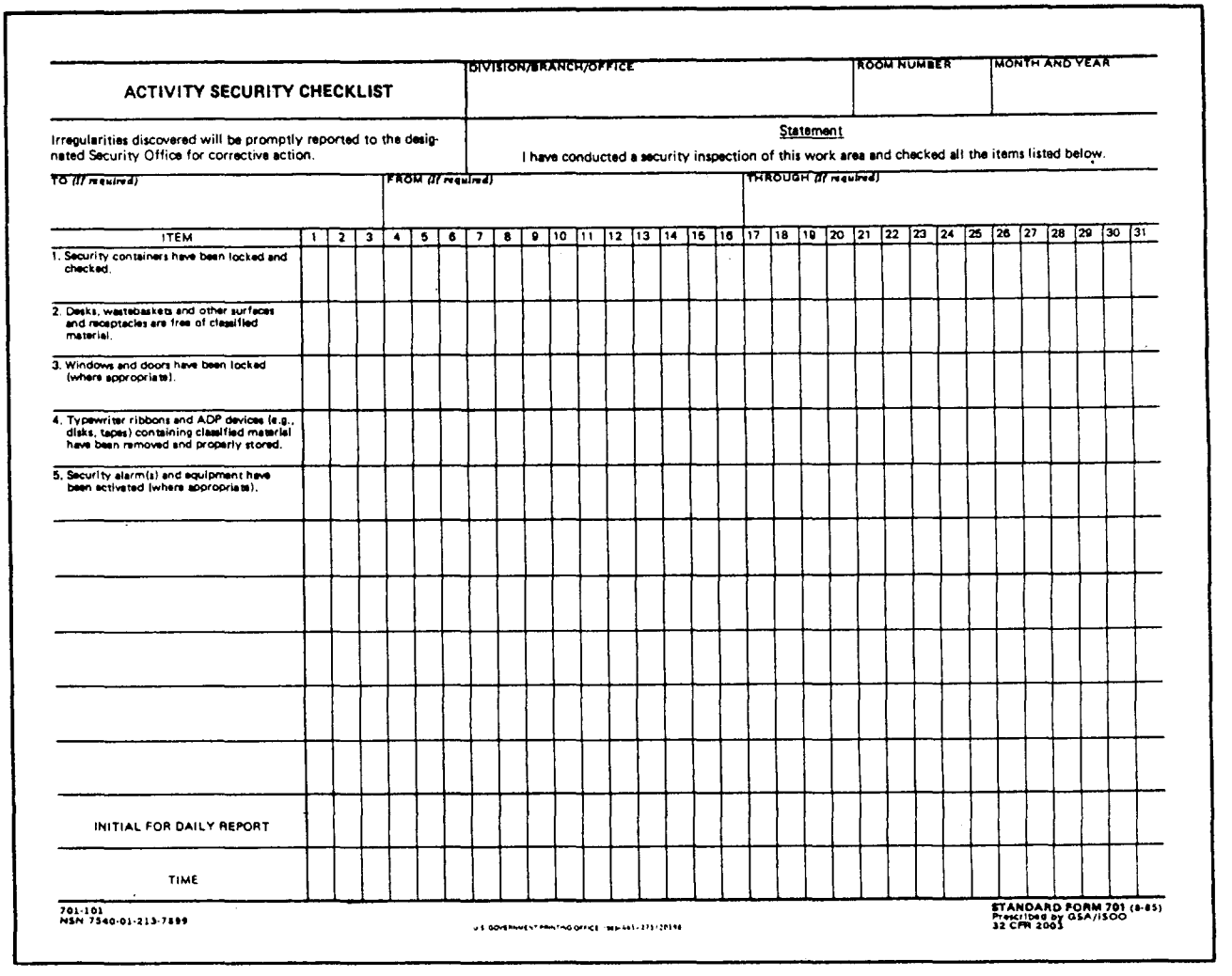
1. If the upper and lower sections have been cycled through the machine five times in the course of regular typing
2. If it is a fabric ribbon, even if it is later used for classified work
3. If it remains stationary in the typewriter for at least five consecutive impressions

Place an Activity Security Checklist, Standard Form 701 (fig. 9-8), in security areas to help you safeguard classified material.

Storage Requirements

Commanding officers are responsible for the safeguarding of all classified information within their commands. That includes ensuring classified material is either in use or under the personal observation of cleared persons as authorized by OPNAVINST 5510.lH.

Figure 9-9 charts the requirements for protecting classified material in storage. Report any weakness or deficiency in equipment being used to store or safeguard classified material to OP-09N. Fully describe the problem and how you discovered it.



ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

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

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

701-101
NSN 7540-01-213-7899

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

Figure 9-8.-Activity Security Checklist, Standard Form 701.

	SHORE INSTALLATIONS			SHIPS			AIRCRAFT		
	TS[1]	S	C	TS[1]	S	C	TS[1]	S	C
CLASS "A" VAULT	X	X	X						
CLASS "B" VAULT	X[2]	X	X						
STRONGROOM	X[3]	X[2]	X	X[5]	X[2]	X	X[5]	X[2]	X
GSA CONTAINER	X[2]	X	X	X[2]	X	X	X[2]	X[4]	X
LOCK BAR CABINET		X[2]	X[4]		X[2]	X		X[2]	X[4]

1. Must be located in buildings, ships, and aircraft which are under U.S. Government control (see definition below); otherwise, must be protected by an alarm system or be guarded during non-working hours by U.S. citizens.
2. Surrounding area locked and access to area controlled by U.S. personnel.
3. Container alarmed or guarded by U.S. personnel.
4. Surrounding area locked.
5. Area alarmed and patrolled every hour by U.S. personnel.

Figure 9-9.-Classified material storage requirements.

Storing valuables, such as money, jewels, precious metals, or narcotics, in the same container with classified material risks the security of that material. Someone could open or steal the container, resulting in the compromise of the information contained in it.

For identification purposes in the event of emergency destruction or evacuation, place a number or symbol indicating its priority on the exterior of each security container: However, conceal the level of classification of the material stored inside the container.

Store Top Secret material in a safe-type steel filing container having a built-in, three-position, dial-type combination lock approved by the General Services Administration. Alarm systems or guards who are U.S. citizens protect storage containers, vaults, or vault-type rooms located in areas or structures controlled by another country.

The physical barrier of an alarmed area used for the storage of Top Secret material prevents the following: (1) secret removal of the material and (2) observation that would result in the compromise of the material. The physical barrier is such that a forcible attack will leave evidence of an attempted entry into the room or area. The alarm system immediately notifies the U.S. security force of an attempted entry.

COMBINATION LOCKS AND KEYS. —The development of the manipulation-proof (MP) and the manipulation-resistive (MR) locks in 1950 advanced security awareness to the point that secure locking devices now exist. A security filing cabinet, vault, or strong room is now fitted with a lock that resists opening of the container by unauthorized persons. This lock is a vast improvement over the antiquated methods of safeguarding before the MP and MR locks were developed.

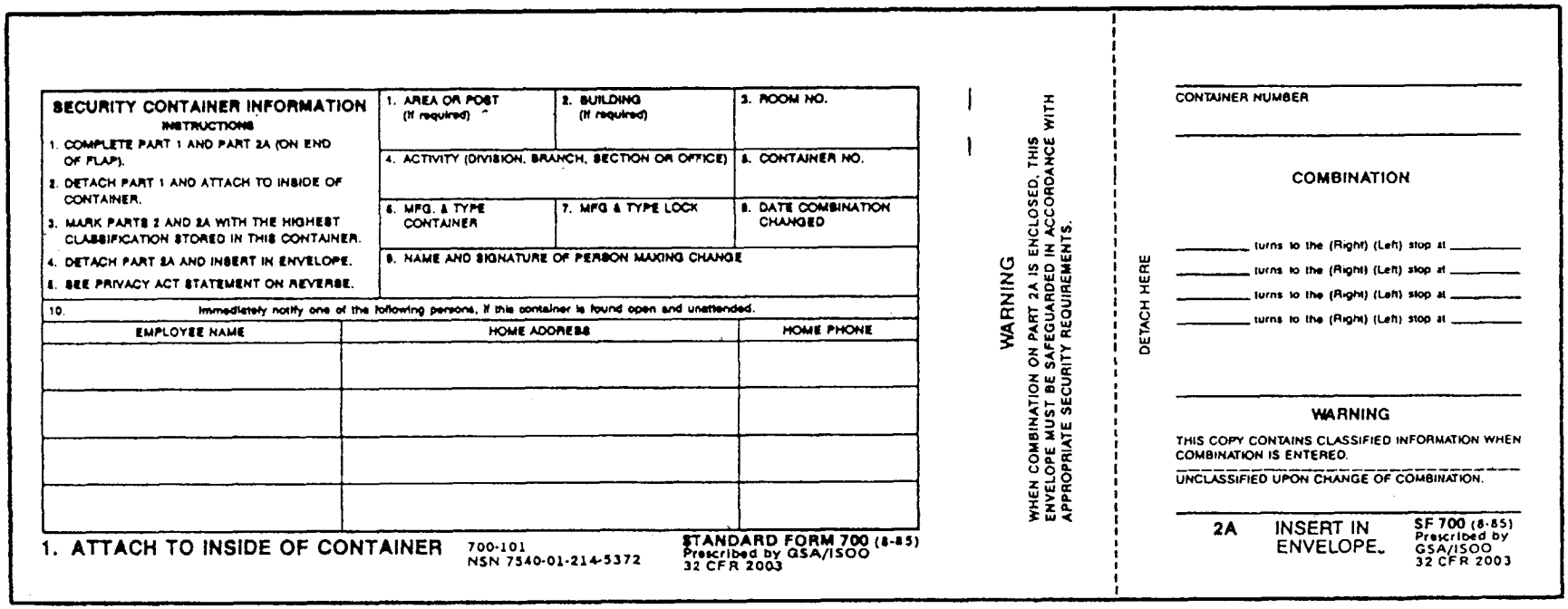
The MP and MR locks have more advanced features designed to protect against expert manipulation than those found in conventional locks. These locks have at least 100 graduations on the dial, which provide a choice of at least 1 million combinations. A three-tumbler lock prevents them from being unlocked when more than one full dial graduation occurs on either side of the proper number for each tumbler wheel.

Federal specifications governing the manufacture of security filing cabinets and security vault doors require that units be equipped with a top-reading changeable combination lock. The top-reading design replaced the front-reading design to provide increased protection against someone getting the combination by secretly watching it being used.

To help ensure the effectiveness of combination locks, comply with the following security requirements:

1. Allow only those persons who are cleared for the highest level of classified material stored in the container to change combinations.
2. Give the combination only to those persons whose official duties demand access to the cent airier.
3. Change combinations when placed in use, at least annually thereafter, and when any of the following occurs:
   a. An individual knowing the combination no longer requires access.
   b. The combination has been compromised or the security container has been discovered unlocked and unattended.
   c. The container (with built-in lock) or the padlock is taken out of service. (When that happens, reset built-in combination locks to the standard combination 50-25-50.) Reset combination padlocks to the standard combination 10-20-30.
4. In selecting combination numbers, do not use multiples of 5; simple ascending or descending arithmetical series; and personal data, such as birth dates and social security numbers.
5. Do not use the same combination for more than one container in any one area.
6. In setting a combination, use numbers that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.
7. To prevent a lockout, have two different people try a new combination before closing the container or vault door.
8. Assign a security classification to the combination equal to the highest category of classified materials authorized to be stored in the vault or container.
9. Seal records of combinations in the envelope provided wit h Standard Form 700 (fig. 9-10), Give the envelope to the security manager, duty officer, communication officer, or any other person designated by the command to keep the records on file.

When key-operated, high-security padlocks are used, control the keys at the highest level of classification of the material being protected.



SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

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

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

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

WARNING

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

DETACH HERE

CONTAINER NUMBER

COMBINATION

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

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN ENVELOPE.

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

Figure 9-10.—Security Container Information, Standard Form 700.

Maintain a record for each vault, secure room, or container used for storing classified materials. Show the location, names, home addresses, and home telephone numbers of the persons having knowledge of the combination. Attach a Standard Form 700, Part 1, to the inside of the container to indicate the responsible custodian.

Electrically actuated locks (for example, cipher and magnetic strip card locks) do not afford the degree of protection required for classified information. The Navy forbids the use of this type of lock to safeguard classified material.

SECURING SECURITY CONTAINERS. — Rotate the dial of combination locks at least four complete turns in the same direction when securing safes, files, or cabinets. Most locks, if their dial has been given only a quick twist, will unlock when the dial is turned back in the opposite direction. Make sure all drawers of safes and file cabinets are held firmly in the locked position after securing them.

After each entry and closure of a security container, document the time opened and time closed. Enter these times and other required information on a Security Container Check Sheet, Standard Form 702 (fig, 9-11).

DESTRUCTION OF CLASSIFIED MATERIAL

Destroy classified material using the method authorized by the instruction governing disposal of Navy and Marine Corps records.

Destroy all classified materials as soon as they are no longer required. Early disposal of

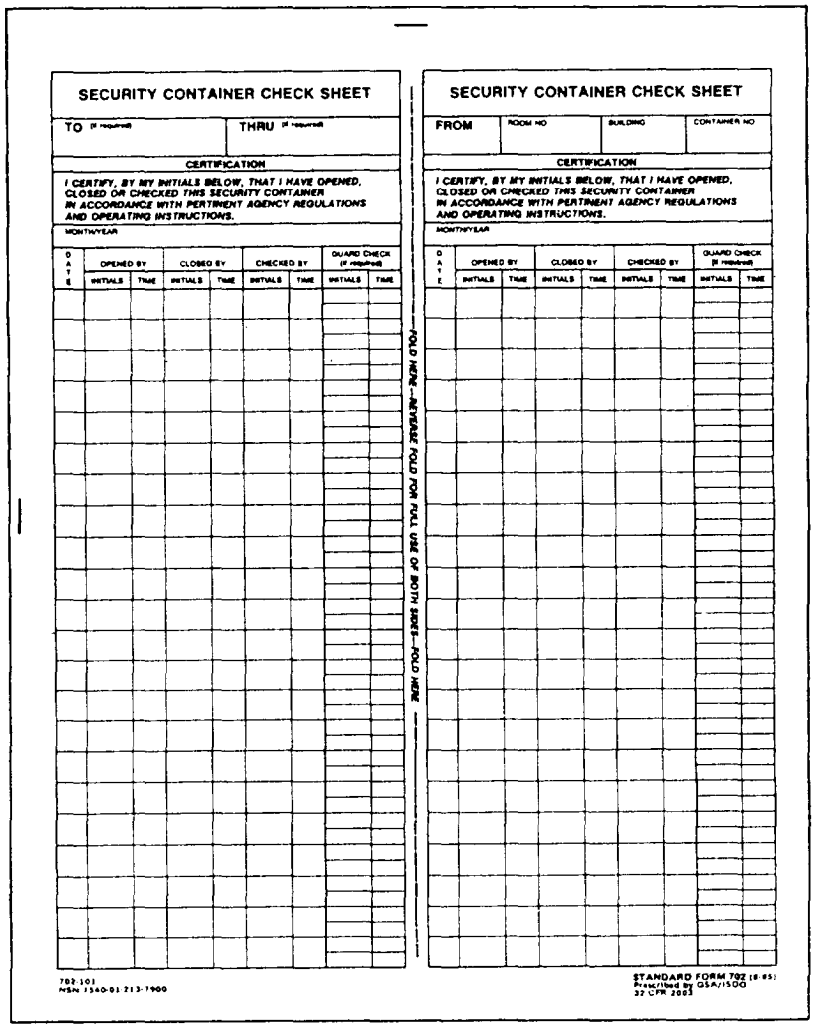


Figure 9-11 .-Security Container Check Sheet, Standard Form 702.

unnecessary classified materials can assist in reducing security costs, preparing for emergency situations, and protecting classified materials.

Destruction Procedures

Destruction of classified material maybe done only by authorized means and by two persons cleared to the level of the material being destroyed.

Give classified material awaiting destruction the same protection you would give the information it contains. Safeguard burn bags at the same level of classification of the materials the burn bags contain until they are completely destroyed.

Record the destruction of Top Secret and Secret materials on the Classified Material Destruction Report, OPNAV Form 5511/12 (fig, 9-12). You may record the destruction on any

CLASSIFIED MATERIAL DESTRUCTION REPORT
OPNAV 5511/12 (REV. 8-76) S/N 0107-LF-055-1100

CLASSIFICATION *(Indicate when title or other identification is classified)*: UNCLASSIFIED

TO: Commanding Officer, USS NEVERSAIL

FROM *(Name and address of activity)*: Top Secret Control Officer

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

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

DESCRIPTION OF MATERIAL

SERIAL/BTS	ORIGINATOR	DATE	COPY NO.	LOG/ROUTE SHEET NO.	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES
00052	CINCPACFLT letter	08/16/87	1	4		4

SAMPLE

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)*: Jon T. Boate

DATE OF DESTRUCTION: 28 Aug 1990

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*: JON T. BOATE GS-12 TSCO

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*: Jack R. Frost JACK R. FROST GS-7

Figure 9-12.-Classified Material Destruction Report, OPNAV Form 5511/12.

other form that includes complete identification of the materials, the number of copies destroyed, and the date of destruction. The two officials responsible for destroying Top Secret and Secret materials will sign and date the record of destruction. Retain records of destruction for a period of 2 years. An originator's statement that a document may be destroyed without report doesn't change the requirement to record the destruction. It only means you don't have to tell the originator the document was destroyed.

The two witnessing officials will sign the record of destruction when Top Secret and Secret materials are actually placed in the burn bag. When the burn bags are destroyed, appropriately cleared personnel should again witness the destruction.

Appropriately cleared personnel may destroy Confidential material and classified waste by an authorized means without recording destruction.

Those personnel destroying classified material do not have to meet any rank, rate, or grade requirements. However, personnel must be familiar with the regulations and procedures for safeguarding classified information.

A command operating a central destruction facility posts the security responsibilities of users and assumes any unassigned responsibilities itself. The central destruction facility may deny users the right to watch the complete destruction of the material or to check the residue after it is burned. In such cases, the central destruction facility is responsible for assuring destruction is complete and reconstruction is impossible.

Methods of Destruction

Burning has been the traditional method for destroying classified material because destruction is complete and disposition of the remaining ash is relatively simple. The remaining ash need only be stirred to ensure destruction is complete and reconstruction is impossible. However, precautions have to be taken to prevent material or burning portions from being carried away by the wind. Incinerators can destroy most types of classified material, but the Clean Air Act has restricted burning. In some areas, state or municipal legislation prohibits burning.

Shredding machines are relatively quiet and require little skill to operate. Shredders vary in their degree of effectiveness, depending on the mechanical condition of the equipment.

The Navy allows the use of two types of shredding machines: the strip shredder and the cross-cut shredder. The strip shredder cuts the material into strips no greater than 1/32 inch in width. The cross-cut shredding machine reduces the material to shreds.

You may shred intermixed classified and Unclassified materials to prevent recognition or reconstruction of the classified material. You may use the strip shredder to destroy classified material and then handle the residue as Unclassified waste except when destroying communications security (COMSEC) and SCI materials.

Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use. The Navy authorizes the use of some pulverizers and disintegrators to destroy photographs, film, typewriter ribbons, glass slides, and offset printing plates. It authorizes the use of others only to destroy paper products.

Use wet-process pulpers to destroy classified water-soluble material. Since pulpers only destroy paper products, make sure you remove staples, paper clips, and other fasteners to prevent clogging of the security screen.

Destroy microform by using an incinerator (where permitted by local environmental regulations) or a shredder approved for the destruction of classified microform. Aboard ships at sea, you may also destroy classified microform (except COMSEC and SCI materials) by cross-cut shredding provided the shreds are no larger than 3/64 inch by 1/2 inch. You may then throw the shreds into the ship's wake.

Unclassified messages and materials, including formerly classified materials that have been declassified, do not require the assurance of complete destruction. Normally, do not destroy Unclassified materials by the classified material destruction system. However, the commanding officer or higher authority sometimes may approve its use because of unusual security factors or for efficiency. One exception is the destruction of Unclassified naval nuclear propulsion information (NNPI). If possible, destroy these materials by methods authorized for destruction of classified material. If not possible, use an alternative that provides a reasonable degree of control during and after disposal. Specific methods depend on local conditions, but the method used should protect against unauthorized recovery of naval nuclear propulsion information (NNPI).

Contrary to widespread opinion, no security policy exists requiring destruction of Unclassified messages (except NNPI). Some telecommunications

and major distribution centers have high volumes of classified and Unclassified message traffic. These centers may find that destroying all messages and intermingled files as if all the information were classified is more efficient. Some units, such as commands located in foreign countries or ships operating in foreign waters, need to take extra precautions in disposing of accumulated message traffic. However, the method of destruction is left to the discretion of the commanding officer. The commanding officer may authorize these messages to be torn into small pieces (as with For Official Use Only [FOUO] material), defaced before discarding, or destroyed by classified destruction methods.

Emergency Destruction

All commands located outside the United States and its territories, those capable of deploying, and those holding COMSEC materials must address the destruction of classified information in their command emergency plan. They must conduct emergency destruction drills periodically to ensure personnel are familiar with the plan and associated equipment.

Commands should take into account the following factors to develop practical, reasonable emergency destruction plans:

- Volume, level, and sensitivity of the classified material held by the activity
- Proximity to hostile or potentially hostile countries with unstable governments and the degree of defense the command and readily available supporting forces can provide
- Flight schedule: or ship deployments in the proximity of hostile or potentially hostile environments
- Size and armament of land-based commands and ships
- Sensitivity of operational assignment (Contingency planning should also be considered.)
- Potential for aggressive action by hostile forces

The emergency destruction plan emphasizes the procedures and methods of destruction personnel must use. It clearly identifies the exact location of all classified materials. It includes priorities for destruction, billet designations of personnel responsible for the destruction, and the prescribed place and method of the destruction. If more than one activity will use a particular destruction site or piece of equipment, the plan sets priorities for its use. The equipment used for routine destruction of classified material is a major factor in the development of the emergency destruction plan.

The plan names the person who will make the decision to begin emergency destruction. It also specifies how this decision will be communicated to all other elements or units maintaining classified information.

The plan also assigns priorities for emergency evacuation and destruction of classified holdings. Priorities are based on the potential effect on the national security should holdings fall into hostile hands.

The priorities for emergency destruction are as follows:

- Priority One—Top Secret material
- Priority Two—Secret material
- Priority Three—Confidential material

Reporting Emergency Destruction

Accurate information about the extent of emergency destruction of classified material is second in importance only to the destruction of the material itself. Report the facts surrounding the destruction to the Chief of Naval Operations (OP-09N) and other interested commands by the quickest means available. Include the following information in the report:

1. The items of classified material that may not have been destroyed
2. The items presumed to have been destroyed
3. The items of classified material destroyed
4. The method of destruction

Additionally, write a statement describing the character of the records and when and where the destruction was accomplished. Submit the statement to the Commander, Naval Computer and Telecommunications Command, within 6 months after destruction.

Commands include the requirement for reporting of emergency destruction of classified material as part of their emergency plan.

DISSEMINATION OF CLASSIFIED MATERIAL

Commanding officers establish procedures to distribute classified material originated or received by commands. They also establish procedures to limit outside distribution to those activities having a need to know and to reflect any restrictions imposed by originators or higher authority.

Review material prepared for public release to ensure it reveals no classified or sensitive Unclassified information. SECNAVINST 5720.44A outlines the policies and procedures governing public release of official information and the conditions under which a security review is required. Certain categories of information require review and clearance by the Assistant Secretary of Defense (Public Affairs).

Top Secret Material

Top Secret material originated within DOD can be disseminated outside DOD only if the originating department or agency gives its consent.

Secret and Confidential Material

Originators may prohibit the dissemination of their classified materials. Otherwise, you may disseminate Secret and Confidential materials to other departments and agencies of the executive branch of the government.

Naval Nuclear Propulsion Information

The protection of all strategically important information is essential to national security. However, because nuclear-powered ships and the naval nuclear propulsion program are major deterrents to war, information about them is a target for hostile intelligence organizations. Therefore, commands need to maintain rigid control over all information about these subjects, whether classified or Unclassified. Unnecessary dissemination, cursory security review, and careless handling of this information help hostile agents in their collection of intelligence.

MARKING OF CLASSIFIED MATERIAL

Classified markings and annotations or other means of identifying classified information reveal the classification level and degree of protection required for material. They also show the level of protection required for extracted and paraphrased information and help to determine the need to downgrade and declassify material. Therefore, mark all classified materials in a manner that leaves no doubt about the level of classification assigned. Use classification markings that leave no doubt as to which parts contain or reveal classified information or how long the materials should remain classified. Take any additional measures needed to protect the materials.

The word *document,* as used in this text, means publications, correspondence (such as military and business letters and memoranda), and other printed or written products (such as charts and maps). Although you can easily mark most documents, you may have difficulty marking materials such as hardware, recordings, and photographs. If the makeup of materials prevent you from marking on them, affix the markings by means of a tag, sticker, decal, or similar device. Affix classification markings so that they are obvious on documents and other types of materials, including containers for storage.

Classified marking and application requirements vary, depending on the kind of material to which you must apply the markings. Include the following basic markings on all classified materials:

- The identity of the original classification authority
- The agency or office of origin
- The overall classification
- The declassification date or event or the notation "Originating Agency's Determination Required (OADR)"
- Any downgrading instructions

The overall classification is the highest classification of any information contained in or

revealed by the material. Overall markings consist of the following:

The overall classification of the material

The most restrictive downgrading/declassification instructions applied to any information in the material

All warning notices or intelligence control markings that apply to information in the material

The classification authority, the office of origin, downgrading and declassification instructions, warning notices, and intelligence control markings are referred to as associated markings.

Figures 9-13 through 9-18 show the correct marking procedures for classified material. Table 9-1 is a detailed marking guide for publications and correspondence.

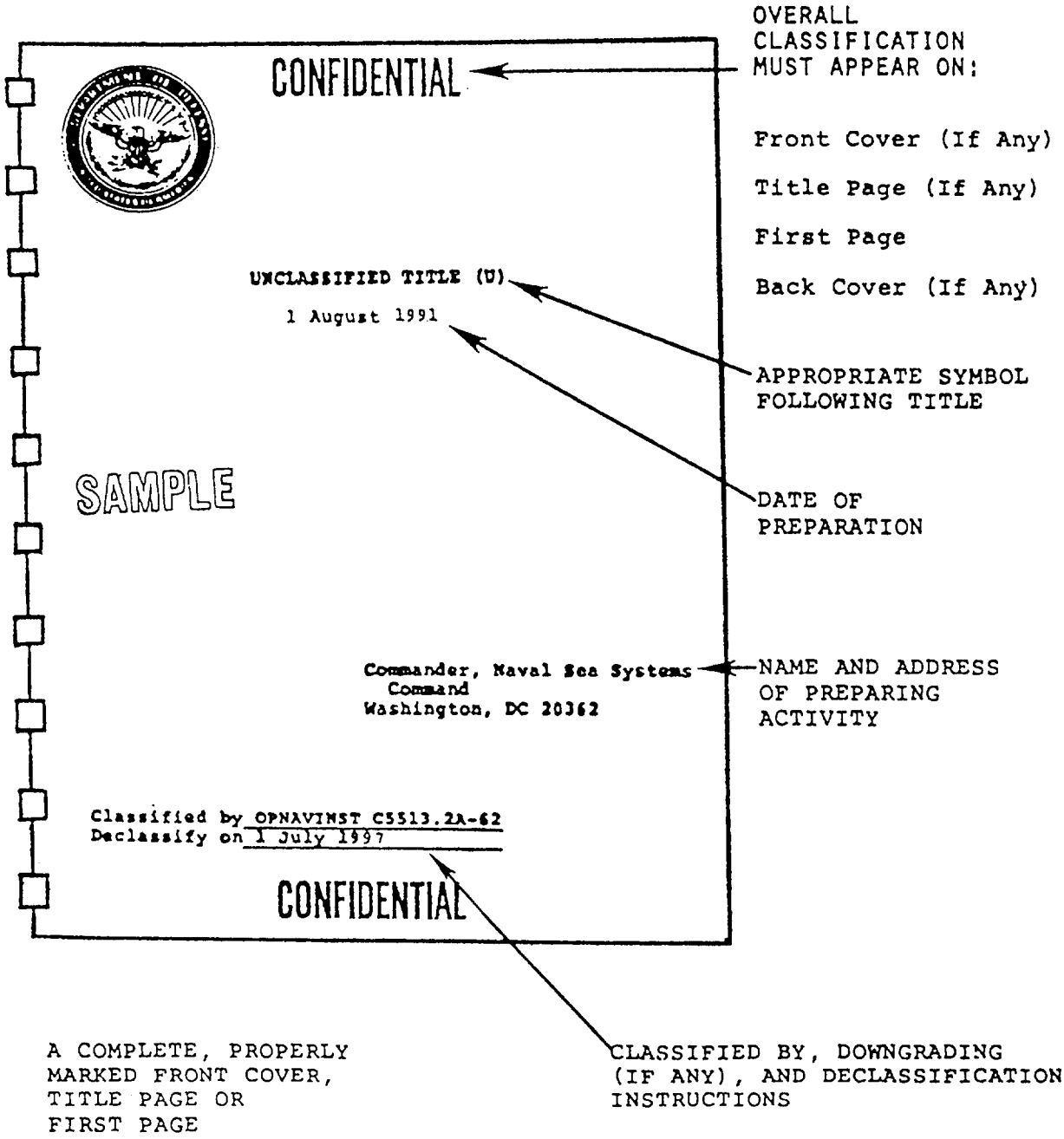


Figure 9-13.-Cover of a publication.

SECRET

CHAPTER 5

SAMPLE

FIRST ORDER HEADING (U)

Second Order Heading (U)

A. (U) Summary

1. (S) The classification marking of headings is illustrated above. Headings are marked according to their own classification and do not reflect the overall classification of the material which follows. Once a heading is identified by some means, it becomes a paragraph for marking purposes, e.g., "A. (U) Summary", as shown.

2. (U) The classification marking of paragraphs and subparagraphs is the same as for naval letter format. The classification of the lead-in portion of a paragraph is shown at the beginning of the paragraph even though a subparagraph may reveal a higher or lower level of classification

a. (C) Subdivisions need not be marked if they do not express a complete thought. As an example, the following do not express complete thoughts:

(1) Systematized digital projection

(2) Compatible organizational flexibility

(3) Synchronized transitional contingency

b. (U) Individual paragraphs are classified according to the information they reveal.

SECRET

Figure 9-14.-Interior pages of a document.

Table 9-l.-Marking Guide for Publications and Correspondence

MARKINGS	PLACEMENT
*Classification - TOP SECRET, SECRET OR CONFIDENTIAL	On publications, stamped or printed TOP and BOTTOM center in letters larger than other print, preferably in red, on the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). If the back cover is not used, classified text may not appear on the back of the last page. Mark interior pages of publications either with the overall classification or with the classification of the individual page. When exercising the individual page option in cases of front and back printing, both sides of the page must be marked with the highest classification of either side. The side with the lower classification should be indicated at the bottom with the statement "This page is Unclassified" or other classification as appropriate. On the first page of correspondence, typed at the upper left in addition to the markings described above.
*CLASSIFIED BY (Insert) Insert the identity of the original classification authority or derivative classification source. (OPNAVINST 5510.1G lists original classification authorities; classification guides or other classified documents are derivative sources.) If more than one source is used, insert the phrase "Multiple Sources" and list all sources on the official record copy.	Once at lower left on the covering (first) page.
*DECLASSIFY ON (Insert date or event or "OADR") Insert the declassificaation date or event. If neither of these can be predetermined, insert the notation "Originating Agency's Determination Required" or its abbreviation "OADR".	Once at lower left on the covering (first) page beneath the "CLASSIFIED BY" line.
DOWNGRADE TO (Insert classification level) ON (Insert date or event)	Once at lower left on the covering (first) page above the "DECLASSIFY ON" line.
(UNCLASSIFIED) (SECRET) or (CONFIDENTIAL) UPON REMOVAL OF ENCLOSURE (or specific enclosure, as applicable) This marking is required on letters or documents of transmittal which cover enclosures of a higher classification.	Top left following classification marking (the classification marking must equal the highest classification of any enclosure being transmitted). Mark second and succeeding pages at TOP and BOTTOM center with the classification of the transmittal letter or document itself; if it is unclassified, no marking is required.
*AGENCY AND OFFICE OF ORIGIN (required if not otherwise evident).	Once on the covering (first) page.
DATE OF ORGIN	Once on the covering (first) page.
(U), (C), (S), (TS) (required for all paragraphs, subparagraphs, titles, headings, captions, etc.) Naval nuclear propulsion information (NNPI) will not be portion marked.	Before each paragraph or portion (except NNPI), and before each caption. After headings and titles. (Use unclassified titles whenever possible to facilitate indexing.)
*CLASSIFIED BY DOE-DOD classification guide CG-RN-1 dated January 1977. DECLASSIFY ON: Originating Agency's Determination Required. This document shall not be used as a derivative classification source (required marking for NNPI).	Once on covering (first) page.

*Required Marking

Table 9-1.-Marking Guide for Publications and Correspondence-Continued

WARNING NOTICES	PLACEMENT
A RESTRICTED DATA This material contains Restricted Data as defined in the Atomic Energy Act 1954. Unauthorized disclosure subject to administrative and criminal sanctions (Full notice), RESTRICTED DATA (Short form), RD (Abbreviated form).	A Full notice at lower left on the covering (first page) beneath the "CLASSIFIED BY" line, in lieu of a "DECLASSIFY ON" line. Short form typed after classification at the top left on the first page of correspondence. Abbreviated form following portion marking classification symbol, e.g., (S-RD) or (S-FRD).
FORMERLY RESTRICTED DATA Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, Atomic Energy Act of 1954 (Full notice), FORMERLY RESTRICTED DATA (Short form), FRD (Abbreviated form).	
B Special Handling Required - Not Releasable to Foreign Nationals (Full notice) NOFORN (Short form) (May be applied to naval nuclear propulsion information (NNPI) only.) NOTE: An abbreviated form is not used because NNPI is not portion marked.	B On publication, full notice at lower left on the covering (first page). On correspondence, full notice typed after the classification at upper left. Short form to identify tables, figures, charts, etc. Abbreviated form following the portion marking classification symbol, e.g., (S-RD) (N).
Critical Nuclear Weapons Design Information. DOD Directive 5210.2 applies (Full Notice), CNWDI (Short form), (N) (Abbreviated form).	
C COMSEC Material - Access by contractor personnel restricted to U.S. citizens holding final Government clearance (Applied to COMSEC documents being released to contractors.)	C Once at bottom of covering (first) page.
Reproduction requires approval of originator or high DOD authority.	
Further dissemination only as directed by (insert name of activity) or higher DOD authority.	
This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be only with prior approval of the Naval Sea Systems Command (May be applied only to classified or unclassified NNPI.)	

*Required Marking.

Table 9-1.-Marking Guide for Publications and Correspondence—Continued

INTELLIGENCE CONTROL MARKINGS	PLACEMENT
WARNING NOTICE - INTELLIGENCE SOURCES OR METHODS INVOLVED (Full marking) WNINTEL (Short form), WN (Abbreviated form).	Full marking once at bottom center above classification marking on the front cover (if any), title page (if any) and first page of publication. Full marking typed on the first page of correspondence following the classification at upper left. Short form at top or bottom center of applicable pages, and for message classification lines, identification of tables, figures, charts, etc. Abbreviated form following the classification designation in portion marking (e.g., (S-NC)).
NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR CONSULTANTS (Full marking), NO CONTRACT (Short form), NC (Abbreviated form).	
CAUTION - PROPRIETARY INFORMATION INVOLVED (Full marking), PROPIN (Short form), PR (Abbreviated form).	
NOT RELEASABLE TO FOREIGN NATIONS (Full marking, NOFORN (Short form), NF (Abbreviated form).	
THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO (Insert specified country(ies)) (Full marking), REL TO _____ (Short form), REL (Abbreviated form).	
DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (Full marking), ORCON (Short form), OC (Abbreviated form).	

OVERALL AND PAGE MARKINGS FOR CORRESPONDENCE

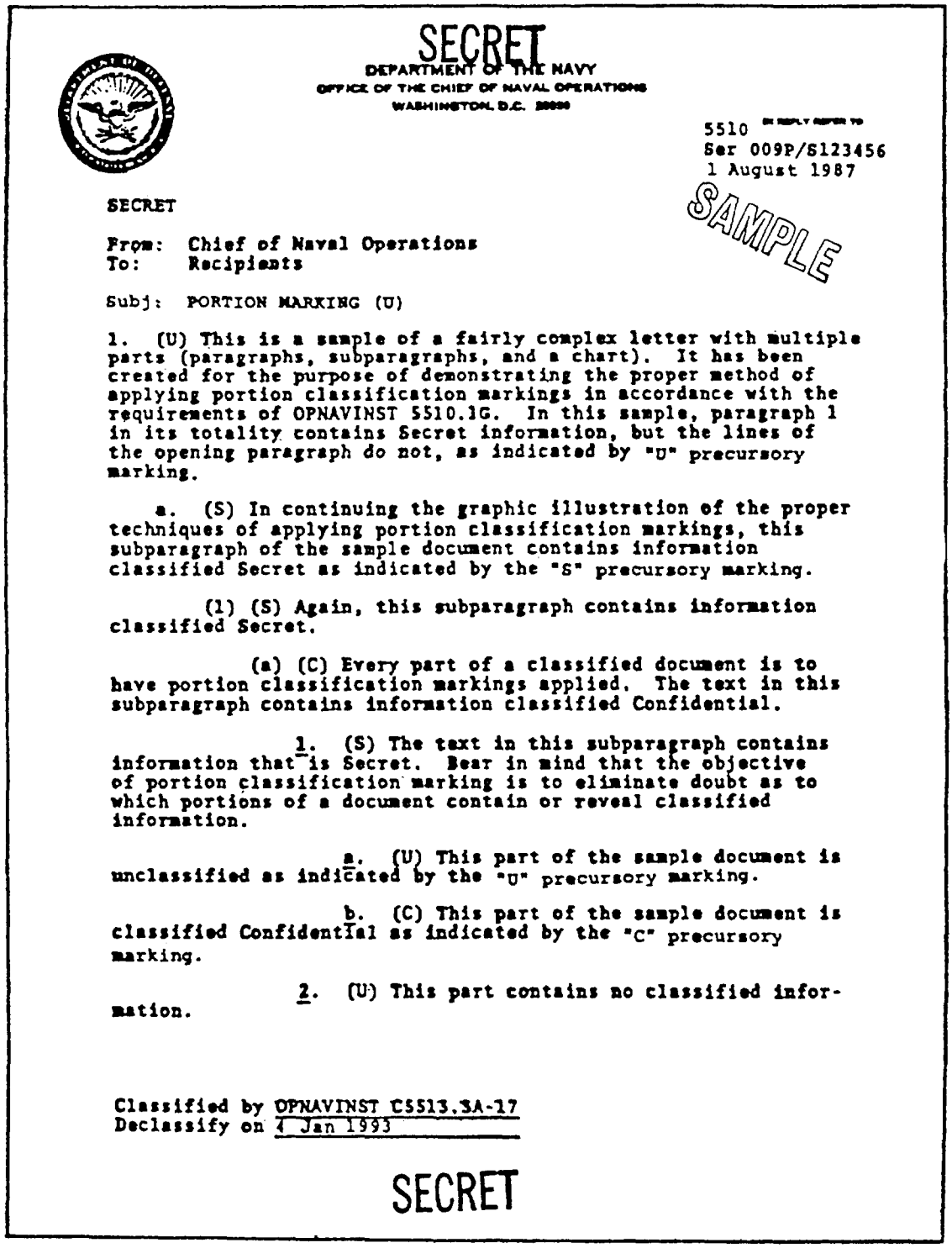
Place the basic markings on the first page of all correspondence (fig. 9-15). Type the overall classification on the first page in the upper left corner and stamp it at the top and bottom center. Place the classification authority and downgrading and declassification instructions in the lower left corner. Spell out warning notices after the typed classification in the upper left corner, except for Restricted Data or Formerly Restricted Data. Type "Restricted Data" or "Formerly Restricted Data" after the classification in the upper left corner and the full warning notice in the lower left corner. Type the intelligence control markings after the classification in the upper left corner.

On the second and succeeding pages, stamp the classification on the top and bottom center. Use either the overall classification or the highest classification of information on that page. Examples of correspondence markings are shown in figures 9-15 and 9-16.

Mark major components of a document, which can be-used independently, as individual documents. Examples are appendices and annexes to plans or operations orders. Always mark an enclosure to a letter of transmittal as an individual document.

Subject and Titles

Whenever possible, use Unclassified subjects or titles of documents to simplify referencing the subject or title in Unclassified documents or indexes. If you need a classified subject to convey meaning, add an Unclassified short title for reference purposes. Mark subjects or titles with the appropriate parenthetical symbol immediately following the subject or title. The parenthetical symbols are (TS) for Top Secret, (S) for Secret, (C) for Confidential, (FOUO) for For Official Use Only, and (U) for Unclassified. When you include the subject or title of a classified document in the reference line, the enclosure line, or the body of a document, follow with a



SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

5510
Ser 009P/S123456
1 August 1987

SAMPLE

SECRET

From: Chief of Naval Operations
To: Recipients

Subj: PORTION MARKING (U)

1. (U) This is a sample of a fairly complex letter with multiple parts (paragraphs, subparagraphs, and a chart). It has been created for the purpose of demonstrating the proper method of applying portion classification markings in accordance with the requirements of OPNAVINST 5510.1G. In this sample, paragraph 1 in its totality contains Secret information, but the lines of the opening paragraph do not, as indicated by "U" precursory marking.

a. (S) In continuing the graphic illustration of the proper techniques of applying portion classification markings, this subparagraph of the sample document contains information classified Secret as indicated by the "S" precursory marking.

(1) (S) Again, this subparagraph contains information classified Secret.

(a) (C) Every part of a classified document is to have portion classification markings applied. The text in this subparagraph contains information classified Confidential.

1. (S) The text in this subparagraph contains information that is Secret. Bear in mind that the objective of portion classification marking is to eliminate doubt as to which portions of a document contain or reveal classified information.

a. (U) This part of the sample document is unclassified as indicated by the "U" precursory marking.

b. (C) This part of the sample document is classified Confidential as indicated by the "C" precursory marking.

2. (U) This part contains no classified information.

Classified by OPNAVINST C5513.3A-17
Declassify on 4 Jan 1993

SECRET

Figure 9-15.-Naval letter.

CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

5510 IN REPLY REFER TO
Ser 009P/C123456
1 August 1991

CONFIDENTIAL

MEMORANDUM FOR RECIPIENTS

Subj: PORTION MARKING SPECIAL FORMATS (U)

1. (U) Mark documents in a manner that eliminates doubt as to which of its portions contains or reveals classified information.

2. (U) There may be occasions when style or format considerations cause an arrangement of words that, standing alone, would not constitute a complete sentence. Normally, such word groups can be revised so as to make a single sentence or paragraph. The following two paragraphs are the same but are arranged differently to illustrate how to apply portion marking.

3. (C) Components of the F-99 aircraft system include:

a. a signal processor;

b. an emitter module;

c. a high frequency receiver; and

d. a cryptographic module.

4. (C) Components of the F-99 aircraft system include a signal processor, an emitter module, a high frequency receiver, and a cryptographic module.

5. (U) Subdivisions of the format in 3 above need not be marked if those subdivisions do not constitute a complete sentence. In the stylized format illustrated, there can be no misunderstanding or doubt that everything would be Confidential when taken together.

F. A. BRUSH
Head, Security Classification
Management Branch
Security Policy Division

SAMPLE

Classified by OPNAVINST S5513.5A-16
Declassify on OADR

CONFIDENTIAL

Figure 9-16.-Memorandum.

similar subject or title classification (fig. 9-17).

Portion Markings

Mark each portion (section, part, paragraph, or subparagraph) of a classified document to show its level of classification or the fact that it is Unclassified. These markings eliminate any doubt as to which portions of a document contain or reveal information requiring protection. However, be sure you consider each portion for classification on the basis of its content and its association with other information. Place the appropriate parenthetical symbol immediately following the portion letter or number. In the absence of letters or numbers, place the appropriate symbol immediately before the beginning of the portion.

When a major numbered or lettered paragraph and all of its subparagraphs are Unclassified, you don't need to mark each paragraph. Marking the lead-in paragraph with a (U) is sufficient.

CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

5510
Ser 009P/C123456
1 August 1991

CONFIDENTIAL--Unclassified upon removal of enclosures (1) and (3)

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

Subj: SECURITY CLASSIFICATION MARKINGS

SAMPLE

Ref: (a) OPNAVINST 5510.1G
(b) CNO Washington DC 012345Z Feb 82

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

1. When titles or subjects of classified documents are included in the reference line, enclosure line or body of the letter, the classification of the title or subject follows, as shown on the enclosure line above. It is not necessary to show the classification of the reference or enclosure itself; however, each classified enclosure which must be removed before the letter of transmittal can be unclassified must be identified at the top, as shown.

2. Only the first page of an unclassified letter of transmittal carries classification markings. There would be no downgrading and declassification instructions on a letter of transmittal which is itself unclassified. If the letter of transmittal contains classified information, it will carry the appropriate downgrading and declassification instructions for the information it contains.

3. Intelligence control markings are typed out in full at the top, following the classification. If any enclosure contains Restricted Data, Formerly Restricted Data or Critical Nuclear Weapons Design Information, the words should be typed out after the classification at the top and the full warning notice placed at the bottom left. If the letter of transmittal contains information classified at the same level as the enclosure but does not, in itself, contain the information requiring the warning notice or intelligence control marking, words to the effect, "Warning notice (intelligence control marking) cancelled upon removal of enclosure (1)" should appear at the top.

JACK R. FROST
By direction

CONFIDENTIAL

Figure 9-17.-Letter of transmittal.

Except in those cases where an intelligence source or method would be revealed, mark portions of United States documents containing foreign government information. Make sure the marking reflects the country or international organization of origin as well as the appropriate classification such as (NATO-S) or (UK-C).

In certain situations, parenthetical portion marking is impractical. In such cases, include on the face of the document a statement that identifies the exact information that is classified and the classification level assigned.

Mark the classification in full, not in an abbreviated form, on figures, tables, graphs, charts, photographs, and similar illustrations incorporated in classified documents. Ideally, you should center the classification marking just below the illustration. Special situations may dictate placement of the marking above or actually within the general area of the illustration. If the information requires a caption, place the abbreviated classification marking for the caption immediately before the text of the caption. When figure or table numbers identify the caption, place the abbreviated marking after the number and before the text.

Transmittals

A transmittal document or endorsement carries the highest classification of the information it transmits. It also contains a statement showing the classification of the transmittal document. An example is an Unclassified letter that transmits a classification of the enclosure and the notation "Unclassified upon removal of enclosure." Also show on the transmittal document any warning notices, intelligence control markings, or special notations on enclosures. Include downgrading and declassification instructions only when the transmittal itself is classified. Otherwise, the notation that the transmittal is "Unclassified upon removal of the enclosure" is the only instruction needed. Figure 9-17 shows a sample of a letter of transmittal.

Electrically Transmitted Messages

Mark classified messages at the top and bottom with the overall classification; also, portion mark as prescribed for other documents. You may use the automated system that prints a message to print the classification markings also, as long as the markings are legible.

Include the overall classification, spelled out, as the first item of information in the text of a classified message. Spell out the identification for Restricted Data, Formerly Restricted Data, or Critical Nuclear Weapons Design Information following the classification; but use the short form for intelligence control markings.

Show the date or event for declassification or the notation "Originating Agency's Determination Required" (fig. 9-18) on the last line of text of a classified, electrically transmitted message.

You may omit the downgrading or declassification annotation on messages containing Restricted Data or Formerly Restricted Data; however, show the basis of the classification on the originator's record copy.

Show the full marking on copies of messages not electrically transmitted (such as mail or courier copies).

Training or Testing Material

Mark classified material used for training or testing purposes and handle as appropriate for that level of classification.

When Unclassified matter is used for training purposes, mark it with the following notation: "(insert the type of classification) for training, otherwise Unclassified." You may purposely mark incorrectly as classified any Unclassified material used to test automated communications systems. Annotate the material as "classified for test purposes only" and handle as Unclassified material.

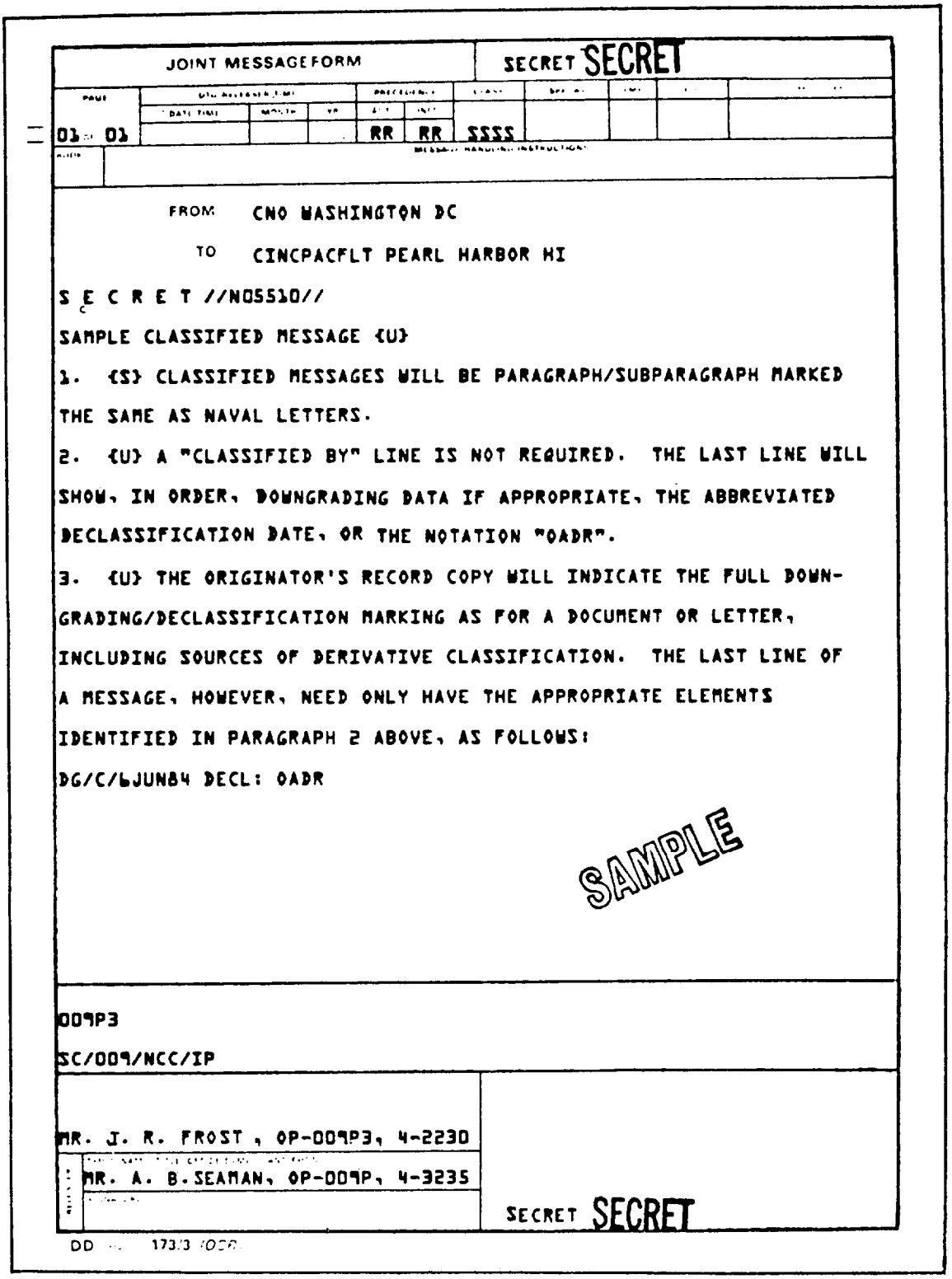
Special Access Program Material

When warranted, material containing information subject to the special access program receives additional marks. Mark special access program material as prescribed in directives, regulations, and instructions relating to approved special access programs. You may change or remove the markings only by direction of the authority responsible for the special access program concerned.

Nuclear Propulsion Information

Classified naval nuclear propulsion information (NNPI) is exempt from the requirements for portion markings.

In documents containing both classified NNPI and other classified information, mark those portions containing classified information other



JOINT MESSAGEFORM

SECRET SECRET

PAGE 01 OF 01

DATE TIME: RR RR SSSS

FROM: CNO WASHINGTON DC

TO: CINCPACFLT PEARL HARBOR HI

SECRET //N05510//

SAMPLE CLASSIFIED MESSAGE (U)

1. (S) CLASSIFIED MESSAGES WILL BE PARAGRAPH/SUBPARAGRAPH MARKED THE SAME AS NAVAL LETTERS.

2. (U) A "CLASSIFIED BY" LINE IS NOT REQUIRED. THE LAST LINE WILL SHOW, IN ORDER, DOWNGRADING DATA IF APPROPRIATE, THE ABBREVIATED DECLASSIFICATION DATE, OR THE NOTATION "OADR".

3. (U) THE ORIGINATOR'S RECORD COPY WILL INDICATE THE FULL DOWNGRADING/DECLASSIFICATION MARKING AS FOR A DOCUMENT OR LETTER, INCLUDING SOURCES OF DERIVATIVE CLASSIFICATION. THE LAST LINE OF A MESSAGE, HOWEVER, NEED ONLY HAVE THE APPROPRIATE ELEMENTS IDENTIFIED IN PARAGRAPH 2 ABOVE, AS FOLLOWS:

DG/C/6JUN84 DECL: OADR

SAMPLE

009P3

SC/009/NCC/IP

MR. J. R. FROST , OP-009P3, 4-2230

MR. A. B. SEAMAN, OP-009P, 4-3235

SECRET SECRET

DD 173/3 /OCR

Figure 9-18.-Message.

than NNPI. Do not mark those containing NNPI. Include the following statement in the body of the document to explain the absence of markings:

> Those paragraphs which are not marked for classification contain naval nuclear propulsion information (NNPI) which is exempt from the requirement for portion marking set forth in the Department of the Navy Information and Personnel Security Program Regulation.

Place the following downgrading and declassification markings on documents containing classified NNPI that is not Restricted Data or Formerly Restricted Data:

> Classified by DOE-DOD Classification Guide CG-RN-1 dated January 1977.
>
> Declassify On: Originating Agency's Determination Required. This document shall not be used as a basis for derivative classification.

Miscellaneous Materials

Treat materials developed in connection with the handling, processing, production and use of classified information in a manner that ensures adequate protection. Such materials include rejected copy, typewriter ribbons, carbons, and similar items. Destroy these materials at the earliest practical time. Omit marks, stamps, or other indications that the recorded information is classified unless needed to ensure its protection.

PERSONNEL SECURITY CLEARANCES

The basic policy of the Department of the Navy Personnel Security Program designates the Chief of Naval Operations (OP-09N) as the official responsible for managing the security clearance program. The CNO (OP-09N) determines policy for granting access to classified material.

Persons are granted access to classified material only if that access is clearly consistent with the interests of national security. Competent authority may determine a reasonable basis for doubting a military or civilian person's loyalty to the government of the United States. If no doubt is determined, a person's loyalty is assumed to be consistent with the interests of national security. This assumption applies to the appointment or retention of civilian personnel in government positions and acceptance or retention of military personnel in the Navy and Marine Corps.

CITIZENSHIP

Only United States citizens are granted access to classified information or assigned to sensitive duties. Sensitive duties are those in which an assigned military member or civilian employee could bring about an adverse effect on the national security. Any duties requiring access to classified information are sensitive duties.

Reference to U.S. citizens in this text includes all U.S. citizens. It includes those who are U.S. citizens by birth, those who are naturalized citizens, and those who are U.S. nationals. Reference to non-U.S. citizens in this text relates to immigrant aliens and foreign nationals. Immigrant aliens are those who have been lawfully admitted to the United States for permanent residence. Foreign nationals are defined, *for security purposes*, as the following:

- Those who are not U.S. citizens, U.S. nationals, or immigrant aliens
- Those immigrant aliens who have failed to become citizens
- Those U.S. citizens or immigrant aliens who represent a foreign government, foreign private interests, or foreign nationals when they are acting in that capacity

With few exceptions, the Navy and Marine Corps will accept only U.S. citizens as officers but will accept immigrant aliens as enlisted. Under a U.S.-Republic of the Philippines agreement, the Navy may enlist nonimmigrant aliens. Enlisted immigrant aliens (and Philippine nonimmigrant aliens) may not enter into ratings or military occupational specialties (MOS) that generally require access to classified information. They are allowed access to classified information or assigned to sensitive duties only when specifically authorized by OP-09N. The Navy and Marine Corps considers all other foreign nationals to be foreign representatives. They are governed by the foreign disclosure policies and procedures in OPNAVINST 5510.48J and OPNAVINST S5510.155C.

VERIFICATION OF CITIZENSHIP

Citizenship status affects the requirements involved in a security clearance investigation. Consider the clearance eligibility and the access a person will be granted before you start that person's security processing. Personnel are required to submit evidence of citizenship to receive a security clearance. However, to retain a clearance at their present level, personnel who hold a current, valid clearance issued by the Navy or Marine Corps are exempt from this requirement. Verification is required for first-time clearance candidates and candidates for clearance at a higher level than currently held if citizenship was not verified previously.

Navy and Marine Corps officers must submit proof of citizenship before their commissioning. Unless a person's record specifically notes that he or she is not a U.S. citizen, you may assume that an officer is a U.S. citizen. Enlistees must submit documentation verifying their citizenship status during enlistment processing.

Civilians must provide documentation proving the citizenship claimed on their application during the hiring process. Never assume a former officer is a U.S. citizen. The former officer must provide evidence of citizenship if the personnel record is unavailable.

The following conditions may satisfy the requirement for a service member to verify U.S. citizenship for a clearance at a higher level than currently held:

1. The person has a valid background investigation (BI) or special background investigation (SBI) completed before 1 September 1979, provided U.S. citizenship was claimed at that time.

2. The person is an officer in the Navy or Marine Corps, although the record does not contain evidence of noncitizenship.

3. An enlisted member's service record contains a DD Form 1966 (Application for Enlistment—Armed Forces of the United States) with a certification that the documents verifying citizenship have been sighted; or for Navy members, a NAVPERS 1070/601 (Immediate Reenlistment Contract) reflecting that the documentation has been sighted and the person is a U.S. citizen.

The following documentation is required to prove U.S. citizenship; it is generally the same as that required for U.S. passport purposes:

1. If the person was born in the United States, a birth certificate is required. A certificate in the form officially issued and certified by the state or county agency is acceptable if it shows the birth record was filed shortly after birth and it bears the signature of the registrar.

a. A delayed birth certificate (a record filed more than 1 year after the date of birth) is acceptable.

b. Verification of birth (DD Form 372) is acceptable for military members if the birth data listed is verified by the registrar.

c. A hospital birth certificate is acceptable if all of the vital information is given and it has an authenticating seal or signature. The hospital must be fully recognized and credentialed by a recognized authority.

d. If primary evidence cannot be obtained, a notice from the registrar that no birth record exists should be submitted. The registrar's notice must be accompanied by the best combination of secondary evidence obtainable. Secondary evidence includes a baptismal certificate; a certificate of circumcision; affidavits of persons having personal knowledge of the facts of the birth; or other documents, such as an early census, school or family bible records, newspaper files, and insurance papers. The secondary evidence should have been created as close to the time of birth as possible.

e. All documents submitted as evidence of birth in the United States must be original or certified copies. Uncertified copies are not acceptable.

2. If citizenship was acquired by birth abroad to a U.S. citizen parent, one of the following is acceptable:

a. Certificate of Citizenship issued by the Immigration and Naturalization Service

b. A. Report of Birth Abroad of a Citizen of the United States of America (Form FS-240)

c. A Certification of Birth (Form FS-545 or DS-1350) issued by a U .S, Consulate or the Department of State

For personnel born in the Canal Zone, a certificate of birth issued by the Canal Zone government indicating U.S. citizenship and

verified with the Canal Zone Commission is acceptable.

3. If the person claims U.S. citizenship by naturalization, a Certificate of Naturalization is required. A Certificate of Citizenship is required if the person claims to have derived U.S. citizenship through the naturalization of the parent(s). If the person does not have a Certificate of Citizenship, the Certificate of Naturalization of the parent(s) may be accepted if the naturalization occurred before the age of 18 (or before the age of 16 before 5 October 1978) and the person was a permanent U.S. resident. Certificates presented must be originals; making copies is illegal.

4. A U.S. passport issued to the person or one in which the person was included (that is, a child and parent on a passport photograph) is acceptable.

PERSONNEL SECURITY INVESTIGATIONS

Persons are given access to classified information or assigned to sensitive duties only if their loyalty, reliability, trustworthiness, and judgment is determined. The initial determination is based on a personnel security investigation (PSI) appropriate to the access required or to other factors involving the sensitivity of the duties assigned.

Although commanding officers may request PSIs on personnel under their jurisdiction, they may request only the minimum investigation to satisfy a requirement.

The Defense Investigative Service (DIS) or, where specified, the Office of Personnel Management (OPM) conducts or controls all PSIs for the Department of the Navy. You are prohibited from conducting PSIs, including local public agency inquiries, without a specific request from DIS.

Keep PSI requests to the absolute minimum. Do not use them as a means of identifying problem personnel security cases.

Types of Personnel Security Investigations

A personnel security investigation(PSI) is an inquiry by an investigative agency into a person's activities conducted for the purpose of making a personnel security determination. Investigations conducted for other purposes may affect a person's employment, clearance, or assignment, but are not PSIs. Examples are investigations of compromise, criminal activity, sabotage, espionage, or subversion.

Because the Navy uses various levels of information, it must have a system of protecting all types of information that could jeopardize our national security. Some materials could have a more devastating effect on our nation than others. For that reason, the Navy conducts personnel security investigations before granting a security clearance to persons who handle sensitive information. These investigations fall into one of the seven categories described in the following paragraphs.

NATIONAL AGENCY-CHECK. —A national agency check (NAC) is a check of federal agency files on persons who apply for employment by federal agencies. The check, conducted by DIS, includes a check of the Defense Central Index of Investigations (DCII) and a check of FBI files. An NAC includes a check on other agencies when the information on the applicant's investigative forms indicates a need for one. The NAC conducted on a first-term enlistee in the Navy or Marine Corps is called an entrance NAC (ENTNAC). The primary reason for an ENTNAC is to determine a person's suitability for entry into the service. It is requested only at the time of *initial* entry, not at reenlistment or at a later date. An NAC is also required for each person accepting a commission in the naval service or a Reserve component commissioned officer status. The NAC is an integral part of each background investigation (BI), special BI (SBI), or periodic reinvestigation (PR). When an NAC discloses information that DIS must investigate further to resolve, the result is called an expanded NAC (ENAC).

NATIONAL AGENCY CHECK AND INQUIRY. —A national agency check and inquiry (NACI) is a check of the files of civilian applicants for employment by federal agencies (an NAC), which includes written inquiries about the applicants. The Office of Personnel Management (OPM) conducts this check. It sends inquiries, covering the person's last 5 years before application, to law enforcement agencies, former employers, supervisors, references, and schools.

DOD NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES. —A DOD national agency check plus written inquiries (DNACI), conducted by DIS, consists of an NAC, credit

bureau checks, and written inquiries to current and former employers covering a 5-year period.

BACKGROUND INVESTIGATION. —DIS conducts a background investigation (BI) to gather information on a person's loyalty, character, emotional stability, and reliability. It consists of an NAC plus a field investigation consisting of an interview and a written inquiry. Standard BI elements include checks of employment; education; organization affiliations; local agencies; where the subject has lived, worked, or gone to school; and interviews with persons who know the individual. Depending on the information disclosed, the BI may also include credit and neighborhood checks and an interview of the subject to resolve any questionable or derogatory information. The scope of a BI usually covers a period that extends back 5 years or begins at the 18th birthday, whichever is the shorter period; however, at least the last 2 years are covered, with the exception that no investigation is conducted before a person's 16th birthday. No time limit is set for the resolution of questionable or derogatory information. The scope of a BI for persons assigned to NATO billets and for non-U. S. citizens is 10 years (with the restriction on investigation before the 16th birthday). A full field investigation (FFI) conducted by the FBI or OPM is the equivalent of a BI.

SPECIAL BACKGROUND INVESTIGATION. —A special background investigation (SBI), conducted by DIS, extends coverage of the person's background to provide a greater depth of knowledge than a standard BI. An SBI includes an NAC on the member's spouse or cohabitant. It also includes an NAC on any immediate family members 18 years of age or older who are U.S. citizens other than by birth or who are not U.S. citizens. The scope of an SBI covers a period that extends back 15 years or begins at the 18th birthday, whichever is the shorter period; however, at least the last 2 years are covered, with the exception that no investigation is conducted before the person's 16 birthday. At the present time, CNO authorizes SBIs only on personnel who have access to certain information or who are assigned to certain duties. The following assignments presently require an SBI:

Assignments requiring access to single integrated operational plan—extremely sensitive information (SIOP-ESI)

Assignments requiring access to sensitive compartmented information (SCI)

Assignment to Presidential support duties

Assignment to investigative agencies as special agents or investigative support personnel requiring continuous access to investigate files and materials

PERIODIC REINVESTIGATION. —A periodic reinvestigation (PR) updates a valid investigation conducted by DIS. It consists of a personal interview, an NAC, local checks, credit checks, and interviews with employment references and character references. A periodic reinvestigation also includes a command review of all available records when warranted by the facts of the case.

SPECIAL INVESTIGATIVE INQUIRY. —A special investigative inquiry (SII), conducted by DIS, has two purposes. The first purpose is to prove or disprove allegations about a person on whom a personnel security determination has been made. The second is to assess the current eligibility of an individual on whom an unfavorable personnel security determination had previously been made. An SII consists of a limited inquiry, a post-judicatory investigation, or some other type of DIS inquiry. SIIs do not investigate current criminal activity, sabotage, espionage, or subversion. The Naval Security and Investigative Command investigates those matters.

Since SIIs supplement the basic PSI, they are not entered as investigations on the Certificate of Personnel Security Investigation Clearance and Access (OPNAV Form 5520/20).

The Nuclear Weapons Personnel Reliability Program

Investigative requirements for the Nuclear Weapons Personnel Reliability Program (PRP) are based on the sensitivity of the position occupied. The position may or may not reflect the classification level of information to which the person may have access. Positions in the PRP are designated as Critical or Controlled.

A Critical position in the PRP requires a BI within the past 5 years before initial assignment. Continued assignment to a PRP position is allowed without an update of the investigation.

A Controlled position in the PRP requires an NACI or DNACI investigation within the past 5 years before assignment. Continued assignment to a Controlled position is also allowed with an update of the investigation.

Initial assignment in the program is interpreted as the first time a person is screened and qualified for the program, regardless of the position occupied. Subsequent assignments in the PRP require a reinvestigation under the following conditions:

1. When the person has been out of the program more than 5 years
2. When the requirements for the PRP position currently being considered have not been satisfied by an investigation within the last 5 years

When military personnel have a break in active duty of more than 1 year, investigations completed before the break become invalid for assignments to the PRP. However, they may be used to determine if a person is eligible for a clearance. Included are persons who transfer from active duty into the Reserves for over a year and then return to active duty. An investigation completed in the previous tour of active duty is also invalid for PRP assignments.

ACCESS TO CLASSIFIED MATERIAL

The Department of Defense uses the simple principle of circulation control to maintain security of classified information. Circulation control means that knowledge or possession of classified information is permitted only by persons requiring access in the interest of national security. Only personnel who are eligible are granted access.

No one is granted access to classified information solely because of rank, position, or a security clearance. The person authorized to have possession, knowledge, or control of classified information has the final responsibility for deciding whether a person requires access to that information.

The preceding security precautions also apply to access by another federal agency, a defense contractor, a foreign government, or an organization such as a command.

GRANTING ACCESS

Commanding officers have the authority to grant access to classified information and are responsible for the security of the information or materials in their command. They may grant access to classified information to persons who have an official need to know or a valid security clearance. They may also grant access if local disqualifying information is unavailable about a person.

The commanding officer should take the following steps in granting access to a member of a command:

1. Determine the level of access necessary for the person to perform his or her official duties (need to know).
2. Check the person's official personnel record and determine if he or she has, or is eligible for, the proper clearance.
3. Review the available command records and reports for possible disqualifying information.
4. Grant the access and record it if the person has the proper clearance and, disqualifying information is unavailable.

Since granting access is a command responsibility, access is terminated automatically when the person transfers from the command, is discharged, or is separated from federal service. It is also terminated when a security clearance is withdrawn, denied, or revoked for any reason.

When questionable or unfavorable information becomes available on a person who has been granted access, commanding officers may decide to restrict or suspend access. They may use a restriction or suspension of access *for cause* only as a temporary measure until the person's eligibility for access is resolved.

LIMITED ACCESS AUTHORIZATION

Commanding officers may sometimes grant access to classified information to a person who is ineligible. The person maybe someone outside the executive branch of the government or someone who is otherwise ineligible for a security clearance. Commanding officers may grant such access only in the interest of national security. Those commanding officers who decide to grant access to such a person should submit a request to CNO (OP-09N) for a limited access authorization (LAA). The CNO (OP-09N) will accept LAA

requests only from active-duty commanding officers. When OP-09N grants an LAA, commanding officers then assume responsibility for briefing the person. They also have the responsibility of limiting the person's access to that information authorized and debriefing the person at the end of the access period.

The CNO (OP-09N) will authorize access only for the specific purpose and the specific classified information stated in the request. In the case of non-U. S. citizens, the information requires release from the country of origin. The authorization will be effective for the period of time necessary, subject to reinvestigation every 5 years. Physical custody of classified material is normally refused. Unlike a security clearance or a command-granted access, an LAA is not entered on the Certificate of Personnel Security Investigation, Clearance, and Access.

ACCESS BY RESERVE PERSONNEL

Reserve personnel who have an appropriate clearance may be granted access to classified information for active-duty training or inactive-duty training. The clearing authority or the authority with the information to be disclosed determines the need for access. Access granted for inactive-duty training should be recorded on the Certificate of Personnel Security Investigation, Clearance, and Access.

Inactive Reserve personnel are ineligible for access to classified information unless they are specifically authorized by OP-09N under limited clearance procedures.

Reserve personnel are granted access to training editions of the following documents as required to maintain proficiency in their specialties:

Codes
Cipher systems
Authentication systems
Call-sign encryption systems
Operation instructions
Maintenance manuals

They are also granted access to COMSEC publications listed as study materials for advancement in rate. Additionally, selected units are authorized access to operational COMSEC materials. Properly cleared inactive-duty personnel taking part in unit drills with these selected units are given access to COMSEC materials as required in the performance of their duties.

ACCESS BY RETIRED PERSONNEL

Retired personnel, including those on the temporary disability retired list, are not entitled to access to classified information because of their present or former status. Commanding officers grant retired personnel access to classified information only when it will promote national security. Commanding officers may submit a request for access authorization to OP-09N.

RECORDING ACCESS

Record access granted by a command, preferably on the Certificate of Personnel Security Investigation, Clearance, and Access, OPNAV Form 5520/20. The commanding officer or his or her designated representative must sign all access entries.

The commanding officer makes certain the Comments section of OPNAV Form 5520/20 contains any access restrictions that apply to personnel.

ADP SECURITY

Automated data processing (ADP) security is a Navywide responsibility. It includes security aspects that contribute to the protection of the total ADP activity, office information system, or network. It involves the following elements:

- Physical security, administrative procedures, operating procedures, and personnel
- Communications and emanations
- Hardware, software, and data

The level of data processed by an ADP activity or network and the cost of carrying out an ADP security program require careful management of ADP security. All Department of the Navy (DON) activities must regularly review and continuously monitor their ADP security program.

The ADP security program will protect ADP activities, office information systems, and networks and the data they process as outlined in appropriate directives.

Refer to the ADP Security *Manual,* OPNAVINST 5239.1A, for a thorough description of ADP security policies and procedures.

SUMMARY

As you advance in rate to chief petty officer, your responsibility to your subordinates and to your country increases. By the time you have attained the rate of petty officer first class or chief petty officer, the Navy realizes you have matured and can accept more responsibility. That is apparent when your division officer or department head shares schedule changes or other sensitive information with you so that you can adjust your divisional work schedule.

This chapter is only an introduction to the security requirements you are responsible for enforcing. You will find specific security requirements in the *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1H.

You, the experienced first class or the seasoned chief, will teach your junior personnel the details of the security program. Therefore, you need to know the Navy's basic security requirements and be aware of those actions considered as security violations. Your life and the lives of your shipmates may depend on information that could fall into the hands of a hostile country. Report any counterintelligence matters to a Naval Investigative Service office.

You will be responsible for marking proper security classifications on classified correspondence. Many of these markings are also used in the marking of classified publications. You need to understand the different personnel clearances and the required investigations for each. Remember that the necessity for access to classified information rests not with the person needing it, but with the person holding the material. You must consider the best interests of both the nation and the Navy in making intelligent decisions regarding access to classified material.

Remember, that stranger who is inquisitive about your work during a friendly conversation could be an enemy agent. Be careful to avoid discussions from which anyone could gather information that could risk our national security. A conversation of this type could be your last if you unknowingly divulge classified information to an enemy agent.

REFERENCES

ADP Security Manual, OPNAVINST 5239.1A, Office of the, Chief of Naval Operations, Washington, D.C., 1982.

Department of the Navy Information and Personnel Security Program Regulation, OPNAVINST 5510.1H, Office of the Chief of Naval Operations, Washington, D.C., 1984.

Standard Organization and Regulations of the Navy, OPNAVINST 3120.32B, Chief of Naval Operations, Washington, D.C., 1986.

U.S. Navy Regulations, 1990, Office of the Secretary of the Navy, Washington, D.C., 1990.