CHAPTER 10

SECURITY

The security of the United States in general, and of naval operations in particular, depends greatly upon the success attained in safeguarding classified information. Every communicator must be security conscious to the point that he automatically exercises proper discretion in the discharge of his duties and does not think of security of information as something separate and apart from other matters. In this way, security of classified information becomes a natural element of every task and not an additionally imposed burden.

Most of the vast amount of intelligence handled by naval communications passes at some point through the hands of radiomen—data which, if available to an enemy, would enable him to learn the strength and intent of our forces, and to gather a wealth of technical information relating to the procedures and operations of the United States Navy.

Communication personnel use many official documents and publications that relate to such matters as frequencies, call signs, and procedures. Their contents also must be protected, because the more an enemy knows about our communications the better are his chances of deriving intelligence from them.

Rules and regulations on the subject of security do not guarantee results, and they do not attempt to meet every conceivable situation. The law of diminishing returns limits the control measures that can be employed profitably. In administering security it is important that a balanced and commonsense outlook be maintained. Each of us must learn to exercise proper discretion in carrying out our duties so that observing proper security precautions becomes an automatic and integral part of our work.

In official publications, the terms "classified information," "classified material," and "classified matter" have slightly different shades of meaning. Information, for example, may involve a document, or the term may denote an intangible, such as knowledge obtained by word of mouth. On the other hand, material or matter implies a physical element, such as an item of equipment, although either word might also refer to written intelligence. For our purposes, the three terms are synonymous.

CLASSIFICATION

Official information that requires protection in the interests of national defense is limited to three categories of classification that, in descending order of importance, carry the designation of Top Secret, Secret, or Confidential.

TOP SECRET

Top Secret material or information is that of which the defense aspect is paramount, and the unauthorized disclosure of which would result in exceptionally grave damage to the Nation. Such grave damage might consist of, but is not limited to—

1. Leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or her allies, or a war.
2. The compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

SECRET

The classification Secret is limited to defense information or material, the unauthorized disclosure of which could result in serious damage to the Nation, such as jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to national defense, compromising important military or defense plans or technological developments, or revealing important intelligence operations.

CONFIDENTIAL

The use of the classification Confidential is limited to defense information or material, the

unauthorized disclosure of which could be prejudicial to the defense interest of the Nation.

In addition to the usual types of information included within the Confidential category, such as operational reports, frequency and call sign allocations, and technical manuals, Confidential encompasses these personal elements:

1. Personnel security investigations and other investigations that require protection against unauthorized disclosure.
2. Matters and documents of a personal and disciplinary nature, the disclosure of which could be prejudicial to discipline and morale.
3. Documents used in connection with procurement, selection, and promotions of military personnel, the disclosure of which could violate the integrity of the competitive system.

The term Confidential—Modified Handling Authorized identifies certain Confidential matter pertaining to actual or simulated combat or combat-related operations. The term indicates that although the information concerned warrants security precautions, it requires less secure safeguards in stowage and transmission.

BASIS OF CLASSIFICATION

The Department of Defense security formula is based on the premise of circulation control. The higher the classification, the more limited is the distribution of the classified material. Security considerations in all cases take into account the ultimate required dissemination of the information involved.

Documents and information, including extracts therefrom, are classified strictly according to content—not according to their relationship to other classified material. For example, an outgoing message that refers to another classified message need not bear the classification of the referenced message, provided reference is made by means of the TDTG (explained in chapter 2) or other identifying symbols. The classification of the transmitted message depends entirely on the text.

Classified matter bears a single classification—that of its highest component—even though individual pages, paragraphs, or sections of the material are classified differently. Whenever practicable, those portions of a lesser classification than the overall classification are marked appropriately according to content.

NEED FOR PROPER CLASSIFICATION

The Department of the Navy Security Manual for Classified Information, issued by the Chief of Naval Operations, contains examples of the types of material that should be included in each classification category. Unnecessary classification or overclassification must be scrupulously avoided. Any information that requires safeguarding must be assigned the lowest classification consistent with content. A defense classification marking merely indicates that the material so marked requires certain minimum controls and restrictions regarding its accessibility.

Overclassification delays unnecessarily the action on important papers, overburdens security channels and facilities, and detracts from the importance of classification in the minds of all personnel. Furthermore, it can undermine our security system and jeopardize the protection required for important military secrets.

The Security Manual stresses the need for the greatest possible reduction in the number of highly classified documents. As one step in that direction, the manual designates the officials who have authority to assign an original classification. The commanding officer of a ship, for example, may not originate Top Secret material, unless specifically designated, except by derivative authority. Derivative classification authority may be exercised by any official whose duties necessitate classifying material created by him as a result of or in connection with material already classified. Thus, although a unit commander might not have specific authority to originate a Top Secret message, derivative authority permits him to classify as Top Secret a message of reply to a Top Secret communication.

It is important, of course, that an originator assign the security classification that he is convinced the information requires. If such classification is higher than the originator is authorized to assign, he recommends the classification by so marking the material, states his reason for doing so, and refers the material to higher authority.

RESTRICTED DATA

An occasional source of confusion regarding classification is the term Restricted Data. Oversimplifying, any item so marked is concerned with nuclear weapons or the use of

nuclear material, such as in the production of energy. Restricted Data means, in effect, that the information contained in the document is not to be exchanged with foreign nations unless the exchange is specifically authorized by the Chief of Naval Operations (Director of Naval Intelligence).

The confusion arises because documents containing Restricted Data are marked in the same manner as information that is classified. When the marking appears on a classified item, usually it is shown as a conjunctive classification, e.g., SECRET-RESTRICTED DATA. In addition, any item so marked carries the following identification:

RESTRICTED DATA

Atomic Energy Act of 1954.

DOWNGRADING AND DECLASSIFICATION

Any command may downgrade or declassify material that it originates. Available manpower, however, does not justify an administrative process whereby certain personnel periodically scan all the classified files in each command to determine what may be reclassified or declassified. The time element in analyzing the possible ramifications in each case would reach astronomical proportions. The national interest, however, demands that all classified information be made available to the general public when secrecy no longer is of importance or value.

To overcome the problem, the Secretary of Defense established a procedure, based on an Executive Order, for automatically downgrading, or downgrading and declassifying, certain defense information. Instructions were promulgated to the services by a joint Army-Navy-Air Force directive (for the Navy—OPNAV Instruction 5500.40 series) entitled Automatic, Time-Phased Downgrading and Declassification System. The key word is "automatic." Since the original directive was issued, the applicable instructions have been expanded to include defense information originated by or under the jurisdiction of the Federal Aviation Agency (FAA) and the National Aeronautics and Space Administration (NASA). By compliance with the provisions of the system, originators generally are relieved of future concern for the classified aspects of documents or material they produce. At the same time, recipients are advised upon receipt of the material of the downgrading or declassification status of each item of information they receive.

Depending on the contents of the material, all classified information originated or received within the DOD, FAA, or NASA is placed into one of four groups. The assigned category indicates whether an item therein may automatically be declassified at any time in the future, and if so, when. The grouping by category is as follows:

A document assigned to—	
Group 1:	Is completely excluded from automatic downgrading or declassification.
Group 2:	Is Top Secret or Secret material that normally would fall in group 3 or 4, but is individually and specifically exempted from automatic downgrading or declassification because of its sensitive nature.
Group 3:	Warrants some degree of classification indefinitely; it is downgraded at 12-year intervals, but it is not automatically declassified.
Group 4:	Is downgraded at 3-year intervals and is declassified after 12 years.

With few exceptions, classified material is conspicuously marked, on the front cover or on the first page if there is no cover, with an appropriate downgrading and declassification printed or stamped notation. For group 1 items, the notation need not be shown on material or equipment that bears the designation CRYPTO, or on certain communications intelligence material. The notations are as follows:

Group 1:	EXCLUDED FROM AUTOMATIC DOWNGRADING AND DECLASSIFICATION.
Group 2:	EXEMPTED FROM AUTOMATIC DOWNGRADING.
Group 3:	DOWNGRADED AT 12-YEAR INTERVALS; NOT AUTOMATICALLY DECLASSIFIED.

Group 4: DOWNGRADED AT 3-YEAR INTERVALS; DECLASSIFIED AFTER 12 YEARS.

The automatic downgrading and declassifying procedures apply to messages as well as other forms of recorded information. To eliminate transmission volume, the originator includes, at the end of the text, a group abbreviated notation marking (GP-1, GP-2, GP-3, or GP-4) in lieu of one of the notations described in the previous paragraph. The number may be spelled out to avoid transmission errors.

PHYSICAL SECURITY

Physical security has to do with safeguarding classified information by physical means. It includes the designation of security areas, stowage, custody, accountability, transmission, dissemination, and ultimate disposition or destruction. In other words, here we are concerned with methods of preventing unauthorized persons from obtaining physical custody of classified material.

SECURITY AREAS

Spaces that contain classified matter are known as security areas. These security (or sensitive) areas have varying degrees of security interest, depending upon their purpose and the nature of the work and information or materials concerned. Consequently, the restrictions, controls, and protective measures required vary according to the degree of security importance. To meet different levels of security sensitivity, three types of security areas have been established; all such areas are clearly marked by signs reading "SECURITY AREA—KEEP OUT."

Exclusion Area

Spaces requiring the strictest control of access are designated exclusion areas. They contain classified matter of such nature that admittance to the area permits, for all practical purposes, access to such matter.

An exclusion area is fully enclosed by a perimeter barrier of solid construction. All entrances and exits are guarded, and only those persons whose duties require access and who possess appropriate security clearances are authorized to enter.

Limited Area

A limited area is one containing classified information and in which the uncontrolled movement of personnel permits access to that information. Within the area, access may be prevented by escort and other internal controls.

The area is enclosed by a clearly defined perimeter barrier. Entrances and exits are guarded or controlled by attendants to check personal identification. The area may be protected by an automatic alarm system.

Operating and maintenance personnel who require freedom of movement within a limited area must have a proper security clearance. The commanding officer may authorized the admittance of persons who do not have clearances. In such instances escorts or attendants must be used and other security precautions must be taken to prevent access to the classified information located within the area.

Radio central, the message center, relay stations, transmitter rooms, and other communication spaces usually are designated limited areas. When any of these spaces contain on-line cryptographic equipment, however, they are designated exclusion areas.

Controlled Area

A controlled area usually does not contain classified information. It serves as a buffer zone to provide greater administrative control, safety, and protection for the limited or exclusion areas.

Controlled areas require personnel identification and control systems adequate to limit admittance to those having bona fide need for access to the area.

Passageways or spaces surrounding or adjacent to limited or exclusion areas may be designated controlled areas.

STOWAGE

Classified material not in actual use by appropriately cleared personnel or under their personal observation should be stowed to provide protection commensurate with the security interest of the material.

To provide a basis for establishing security protection for the various categories of classified material, a numerical evaluation for classified material in stowage enables any officer responsible for classified material to determine that an adequate level of protection is attained.

The system, covered in detail in the Security Manual for Classified Information, makes use of two tables:

1. A table of numerical equivalents (fig. 10-1), which establishes numerical values for various items that may be incorporated individually or collectively in the stowage protection system.

2. An evaluation graph (fig. 10-2), which establishes minimum levels of required protection based on the classification and the strategic and intrinsic importance of the material concerned.

The application of the numerical evaluation system to an existing stowage security program is as follows:

1. Select appropriate numerical equivalents for each applicable element in the security program, as set forth in figure 10-1, and total them. Assign only one value for each lettered subsection, interpolating as necessary to reflect the existing situation.

2. In figure 10-2 select from the left of the graph a subcategory that best describes the material to be stowed. Moving across the graph to the right to the point of intersection with the diagonal line shows the numerical value that must be equaled if the stowage is to be considered adequate.

CUSTODIAL PRECAUTIONS

All personnel are individually responsible for assuring that knowledge of classified information which they prepare or handle is made available only to persons who have appropriate security clearances and who have clearly established a legitimate need for the information. In view of this, it might be well to mention several custodial requirements that should be borne in mind constantly.

No one may remove classified material from the confines of the command without the approval of the commanding officer or his representative. When classified material is removed, the individual removing it signs a complete list (receipt) that remains on file until he returns the material.

When working with classified documents, take precautions to prevent either deliberate or casual access to the information by unauthorized persons. When the documents are removed from stowage for working purposes, keep them face down or covered when not in use. Visitors not authorized access to the classified information within a working space are received in an outside area. If the space must be vacated during working hours, stow all classified material as at the end of the working day.

During the preparation of a classified document, all preliminary drafts, sheets of carbon paper, stenographic notes, worksheets, and so on must either be destroyed (or placed in the burn bag) immediately after they have served purpose, or be treated and safeguarded in the same manner as the classified information produced from them.

At the close of working hours, a security inspection is made to ensure that users have stowed all classified material, that material to be passed from watch to watch is accounted for, and that burn bags and the contents of wastebaskets containing classified material are properly stowed or destroyed. Custodians include as part of the inspection a check on loose papers such as carbon sheets, written notes, rough drafts, and the like. As a matter of routine, however, these items should be placed in a burn bag immediately after use and not allowed to accumulate or remain adrift.

When securing a safe, file, or cabinet equipped with a combination lock, rotate the dial of the lock at least three complete turns in the same direction. When the dial is given only a quick twist, it may be possible to open the lock merely by turning the dial in the opposite direction. After the equipment is locked, test all drawers to be sure they are held in the locked position.

ACCOUNTABILITY

Except for publications containing a distribution list by copy number, all copies of each Top Secret document and each item of Top Secret equipment are numbered serially at the time of origination: Copy No._____of_____ copies. Each page of a Top Secret document not containing a list of effective pages is numbered:

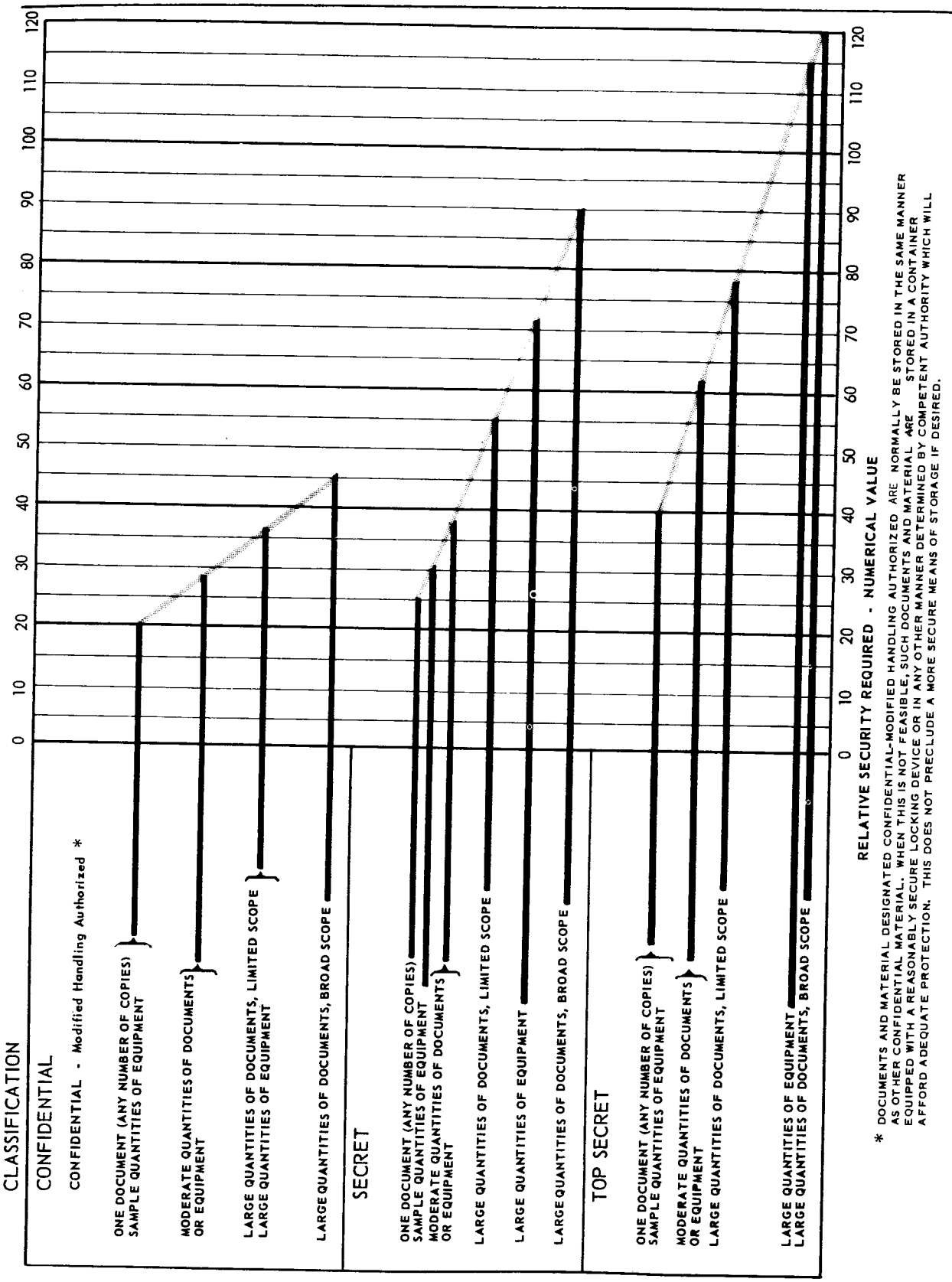
"Page_____of _____pages."

Top Secret documents may be reproduced in whole or in part only with the permission of the originator or higher authority. In the event higher authority grants permission, he should inform the originator immediately. All reproduced copies are numbered serially and recorded with the Top Secret control officer so as

ELEMENT OF SECURITY	VALUE
1. Stowage Areas	
a. Security Fences	
(1) Classified area surrounded by a security fence with all gates secured or controlled	5
b. Protective Lighting	
(1) Security areas lighted by protective lighting	5
c. Building or Ship	
(1) Conventional frame or good quality temporary structure	5
(a) Controlled area within	15
(b) Limited area within	25
(c) Exclusion areas within	35
(2) "In Service" or MSTS chartered Vessel	10
(a) Controlled areas within	20
(b) Limited areas within	30
(c) Exclusion areas within	40
(3) Masonry or steel structure with substantial partitions floors and ceilings (including magazines)	10
(a) Controlled area within	20
(b) Limited area within	25
(c) Exclusion area within	40
(4) Aboard a Commissioned Ship	25
(a) Controlled area	35
(b) Limited area	40
(c) Exclusion area	50
2. Stowage Containers	
a. Portable, any type	0
b. Wood, any type	0
c. Metal, keylock (built-in)	2
d. Metal, keylock (attached)	5
e. Metal, combination bar-lock (attached)	10
f. Metal, combination lock (built-in)	15
g. Light room vault	15
h. Heavy room vault	35
i. Class 3 security filing cabinet, GSA Federal Supply Schedule	50
j. Class 2 security filing cabinet, GSA Federal Supply Schedule	60
k. Class 4 security filing cabinet, GSA Federal Supply Schedule	60
l. Class 5 security filing cabinet, GSA Federal Supply Schedule	70

ELEMENT OF SECURITY	VALUE
3. Guarding	
a. Supporting Guard Force	
(1) Civilian Supporting Guard Force	10
(2) Military Supporting Guard Force	15
b. Guards	
(1) Civilian Guards	
(a) Civilian guard in general area	10
(b) Civilian guard check of container each hour	15
(c) Civilian guard check of container each 1/2 hour	20
(d) Civilian guard in attendance at container	30
(2) Military Guards	
(a) Military guard in general area	15
(b) Military guard check of container each hour	20
(c) Military guard check of container each 1/2 hour	25
(d) Military guard in attendance at container	60
c. Sentry dog accompanying military or civilian guard	10
4. Protective Alarm Systems	
a. Area Alarm System	
(1) Make or break (electromechanical) alarm to detect entry into immediate area	5
(2) Other alarm system to detect entry into immediate area	10
(3) Alarm system to detect entry or attempted entry into immediate area	15
(4) Alarm system to detect entry or attempted entry and approach to immediate area	25
b. Container Alarm Systems	
(1) Make or break (electromechanical) alarm to detect opening of container	10
(2) Other alarm system to detect opening of container	15
(3) Alarm system to detect opening or tampering with container	20
(4) Alarm system to detect opening or tampering with and approach to container	30

Figure 10-1.—Table of numerical equivalents.



31.2

Figure 10-2. — *Evaluation graph.*

31.2

to maintain complete accountability. The copy numbers of reproduced copies should maintain a relationship with the document received originally. For example, if a command holds copy No. 12 of a Top Secret document, and reproduces two additional copies, the latter might be identified as "Copy No. 12/1 of 2 copies" and "Copy No. 12/2 of 2 copies."

A continuous chain of receipts for Top Secret material must be maintained. In addition, a disclosure record form is attached to each document that circulates within a command or activity, and each person having knowledge of its contents signs the form.

Each command establishes administrative procedures for recording all Secret material originated and received, and maintains a receipting system for Secret matter distributed or routed within the command.

Each command also maintains a system that ensures accountability for all Confidential material originated or received.

TRANSMISSION

Classified material must be safeguarded during transmission from one place to another as well as when held within a command. Due to the very nature of the problem, compromise or loss is more probable during transmission than at any other time. For this reason, specific rules ensure maximum security consistent with the need for rapid communication of the information.

Top Secret material may not be sent through any postal system, United States or foreign. It may be transmitted only by one of the following means:

1. Direct personal contact of military personnel (E-7 or above) or appropriately cleared civilians of comparable grade.
2. Armed Forces Courier Service; or
3. Electric means in encrypted form.

Secret and Confidential material may be sent by any of the methods authorized for transmitting Top Secret material, or by U. S. registered mail. (For exceptions, see the next topic on ARFCOS.)

Confidential—Modified Handling Authorized material may be transmitted by ordinary U. S. mail or electrically in unencrypted form over U. S. Government-owned or leased landlines. When the originator is uncertain of the location of an addressee, as a unit afloat, U. S. registered mail must be utilized.

The foregoing rules apply only within the continental United States. When the national boarders must be crossed, the rules are modified slightly. Secret and Confidential matter can be transmitted by U. S. registered mail provided it stays within U. S. military postal channels. Within the continental U. S., Canada, and Alaska, Secret and Confidential may be sent by registered mail with registered mail receipt. Confidential—Modified Handling Authorized may be sent by regular first class mail, which is under the control of the U. S. or Canadian Governments.

Commanding officers are authorized to establish systems for transmitting classified material within the confines of their commands. Such systems must ensure that—

1. Top Secret material always is controlled by Top Secret control officers.
2. Personnel transmitting the classified material have security clearances for the highest category they are allowed to handle.
3. Personnel whose primary duties entail transmission of classified material are authorized in writing for such duties.
4. All personnel entrusted with transmitting classified material are instructed properly concerning their duties.

Armed Forces Courier Service

The Armed Forces Courier Service (ARFCOS) is a joint agency of the three military departments that provides for the secure and expeditious transmission of material, regardless of classification, requiring protected handling by an officer courier. The paramount objective of the ARFCOS is security.

A series of courier transfer stations are set up within the various Navy, Army, and Air Force commands in the United States and overseas. Each transfer station serves the various commands in its area by arranging for the transmission of authorized material originated by or addressed to them. During transit the material normally is placed in custody of a designated courier. The courier is designated by the officer in charge of the courier transfer station, and is called the courier transfer officer. If no qualified officer is available to be designated courier, the courier transfer officer may act in that capacity himself.

A courier ordinarily is designated from among the passengers traveling in a ship, aircraft, or vehicle. Any officer of the armed

Figure 10-2.—Evaluation graph.

services who has written evidence that he is cleared for Top Secret can be designated a courier regardless of the mode of travel. Such evidence of clearance is not required, however, for designation of an officer as a courier for transmission of ARFCOS material on a direct flight between two ARFCOS stations. A specifically designated Department of State courier also may be designated to convey ARFCOS material. Instructions covering the designation of couriers are included in the 2260 series of OpNav Instructions. Suffice it to say that designating as courier an officer who is traveling to the destination of the material ensures the security of the material throughout its transmission. Before departure, the courier inventories and signs for the material from one courier transfer officer and on arrival delivers it to another; or, if he is going to the same destination, he may be ordered to deliver the material directly to the addressee.

The following types of material are authorized for entry into the Armed Forces Courier Service:

1. Top Secret material.
2. Cryptographic material.
3. Cryptologic material (cryptomaterial obtained from an enemy and forwarded for analysis).
4. Registered publication system documents.
5. Communication material that cannot be transmitted electronically because of circuit casualties and is certified to require urgent delivery.
6. Other material approved by the Chief of Naval Operations.
7. Material that cannot be maintained in United States custody by any means except an officer courier.
8. State Department diplomatic pouches.
9. Material of the Central Intelligence Agency.
10. Material of the National Security Agency.
11. Certain NATO, SEATO, and CENTO material as defined in the foregoing items.

DISSEMINATION

"Disclosure," as it relates to classified information, is an officially authorized release or dissemination by competent authority whereby the information is furnished to a specific individual, group, or activity. "Need to know" is the term given to the requirement that the dissemination of classified information be limited strictly to those persons whose official military or other governmental duties require knowledge or possession of the material.

Classified material, to be useful, must be made available to those who need it. At the same time, security demands that classified information not be disclosed needlessly. No person is entitled to knowledge or possession of classified information solely by virtue of his rank, office, or position. Responsibility for determining whether a person's duties require that he possess or have access to any classified information, and whether he is authorized to receive it, rests upon each individual who has possession, knowledge, or command control of the information concerned, and not upon the prospective recipient.

A "need to know" is recognized when these four elements exist:

1. Release of the information is in the interest of national defense.
2. There appears to be a legitimate requirement that the applicant for the material must have the information to carry out his assigned duties.
3. The applicant has no other available source for the information.
4. The applicant is or can be appropriately cleared and is capable of providing adequate protection for the material.

DISPOSITION AND DESTRUCTION

Classified material that is not required should not be allowed to accumulate. It should be sent either to stowage at a naval records management center, or it should be destroyed. The effective revision to SecNav instruction 5212.5 relates the procedures for transferring records. For classified material so forwarded, proper safeguards must be taken to prevent loss or compromise. Extra copies and nonrecord material may be destroyed after they have served their usefulness.

An officer being relieved must deliver to his successor all classified material attached to the command and in his custody. Appropriate receipts cover, as a minimum, all Top Secret and Secret material.

Classified documents are destroyed by burning, pulping, pulverizing, or shredding. Burning is the method used most commonly in the fleet. When destruction is accomplished by

means other than burning, the residue must be inspected to ensure complete mutilation.

When classified papers are burned, the destruction must be witnessed by two commissioned officers. If sufficient officers are unavailable, warrant officers, enlisted men, or civilians may witness the burning, provided they are cleared at least for the highest category of material being destroyed. Witnesses must watch the burning until destruction is complete, after which the residue is obliterated completely by scattering or reduction to sludge. When appropriate, a certificate of destruction is prepared and signed.

In an emergency involving the danger of capture of classified material, it is highly important that such material be destroyed. The ship's emergency destruction bill (fig. 10-3) establishes procedures for the emergency destruction of all classified matter. Responsibility for destruction is assigned by watches, and alternates are provided to allow for casualties. The bill indicates the location of the classified material, the priority of destruction, and the methods of destruction to be employed. The emergency destruction bill is only one phase of a more encompassing emergency plan for security. See RPS 4 and, if available, KAG 1 for more information.

In connection with emergency destruction procedures, ensure that a sufficient supply of destruction materials, such as weighted bags, wirecutters, and sledges (the last two for destroying crypto equipment) are available in all communication spaces. The classified material must be readily accessible at all times for destruction by assigned personnel.

Destruction plans require the highest degree of individual initiative practicable under the operating conditions of the ship. Personnel must understand that, in emergency and when required, they are to initiate necessary destruction under the plan without waiting for specific orders.

TRANSMISSION SECURITY

Transmission security is that component of communication security resulting from all measures designed to protect transmission from interception, traffic analysis, and imitative deception. Every means of transmission is subject to interception. In radio transmission, we must assume that all transmissions are intercepted.

Within the requirements of precedence and security, the most appropriate means of transmission should be selected. The generally available means of transmission, in order of security, are these:

1. Messenger;
2. Registered mail;
3. Approved wire circuit;
4. Ordinary mail;
5. Nonapproved wire circuit;
6. Visual;
7. Sound systems; and
8. Radio.

SPEED VERSUS SECURITY

The three fundamental requirements of a military communication system are reliability, security, and speed. Reliability is always paramount. Security and speed are next in importance and, depending on the stage of an operation, are interchangeable. For instance, during the planning phase, security is obviously more important than speed. During the execution phase, speed surpasses security in importance. This is not to say that either can ever be ignored completely. Modern high-grade cryptosystems permit security with speed. In tactical operations, however, when speed is so important that time cannot be spared for encryption and the transmitted information cannot be acted upon by the enemy in time to influence current operations, messages of any classification except Top Secret may be transmitted in the clear over any wire or radio circuit. Each message must be approved and released separately, and any linkage to previously encrypted messages should be avoided. Such transmissions include the word CLEAR at the beginning of the text to indicate the message contains classified material. Upon receipt, the message is marked "Received in the clear" and is handled as Confidential. If the information must be further transmitted, an entirely new message is drafted.

WIRE SYSTEMS

With respect to transmission of classified information, there are two categories of wire systems: approved and nonapproved. These systems include telephone, telegraph, teletypewriter, and facsimile facilities.

The many requirements to be met before designating that a wire circuit is approved are not

USS JOSEPH K. TAUSSIG
DE-1030
EMERGENCY DESTRUCTION BILL

The following Emergency Destruction Procedures for Classified Material held by this command are effective this date: 10 October 19_

Space	Person Responsible	Alternate	Priority of Destruction
Registered publications safe	RPS custodian	Alternate custodian	1. Emergency keying data. 2. TOP SECRET cryptomaterial. 3. Superseded } Key lists, 4. Reserve } rotors, 5. Effective } and strips. 6. Reg. cipher equipment. 7. Maintenance documents. 8. Operating instructions. 9. Remaining cryptomaterial. 10. Registered publications. 11. Nonregistered classified publications.
Cryptocenter	General quarters cryptomember	Crypto-security officer	
Radio I	Supervisor	Circuit operator	1. Aircraft codes; authentication systems; call sign ciphers; recognition signals. 2. Registered publications. 3. Classified records; files. 4. Classified electronic equipment. 5. Classified nonregistered publications. 6. Unclassified publications and electronic equipment.
Radio II	Circuit operator	Radio I JX talker	
Signal bridge	Supervisor	Assistant navigator	
CIC	Supervisor	JOOD	

1. Method of destruction
   a. Deep water (over 100 fathoms)
      (1) Jettison publications in weighted perforated bags.
      (2) Smash crypto equipment beyond recognition if possible and jettison.
   b. Shallow water (less than 100 fathoms)
      (1) Burn publications completely, break up and scatter ashes.
      (2) Smash crypto equipment beyond recognition or reconstruction, taking care to remove all wiring, and scatter component parts over a wide area. Smash remaining electronic equipments so as to render them useless.
2. Record of destruction
   a. All personnel assisting in the execution of this bill will report in writing to the RPS custodian the degree of completion of such destruction. (Use the last watch-to-watch inventory.)
3. Execution of emergency destruction bill
   a. Emergency destruction will be ordered by the Commanding Officer, or, in his absence, by the next senior line officer present. In the event of an emergency, it may be necessary for the personnel designated above to carry out the provisions of this bill without further orders, if their estimate of the situation admits possibility of the loss of the ship.
4. Location of destruction equipment
   a. Sledges, wire cutters, screwdrivers, and weighted perforated bags are located in each communication space.

Approved:

Tolis Lewie, LCDR USN
Commanding Officer

Submitted:

H. T. Crowley, LTJG USN
Classified Material Control Officer

Figure 10-3.—Emergency destruction bill. 76.7

taken up in this text. An approved circuit may be designated as such only by a service Chief of Staff, the Chief of Naval Operations, the supreme commander of a theater of operations, or such officers as they may designate. The number of approved circuits is kept to a minimum consistent with operational requirements. Each approved circuit is rated according to the highest classification of information authorized to be transmitted over it in the clear. Under no circumstances, however, is information classified higher than Secret so transmitted. With the exception of those situations discussed previously, where speed is more important than security, no classified information may be transmitted in the clear over nonapproved circuits.

VISUAL TRANSMISSION SECURITY

The various means of visual transmission, in order of security, are these day and night groups:

Day:

1. Hand flags;
2. Directional flashing light;
3. Panels;
4. Flaghoists;
5. Pyrotechnics;
6. Nondirectional flashing light.

Night:

1. Infrared communication systems;
2. Directional flashing light;
3. Pyrotechnics;
4. Nondirectional flashing light.

Transmission of a classified message in plain language by visual means is authorized only after careful consideration is given to the possibility of interception by unauthorized persons. The aperture of directional flashing light equipment is kept as narrow as possible, and filters are used to reduce the detectable range at night. Under no circumstances are translations of encrypted messages transmitted by visual means. This method subjects the entire cryptosystem to possible compromise.

RADIO TRANSMISSION SECURITY

When a message is transmitted by radio, it sometimes is possible to know a few of the receivers, but all of them never become known. It must be assumed that the enemy receives every transmission. Properly prepared messages using modern cryptosystems may prevent the enemy from understanding the message, but he still can learn a lot. For instance, as the time of a planned operation approaches, the number of messages transmitted increases so markedly that, although the enemy may be unsure of its exact nature, he knows that something will occur soon and he can alert his forces accordingly. Strict radio silence is the main defense against radio intelligence.

The amount of radio traffic is not the only indicator used by the enemy. He can be expected to run statistical studies of message headings, receipts, acknowledgments, relays, routing instructions, and services. Communication experts can learn much about our operations, past and future, from such studies. By means of direction finders they determine from where the messages are transmitted—a valuable aid in their studies.

Although we cannot prevent traffic analysis by the enemy, it can be made more difficult and less reliable. Such measures as the following can be taken:

1. Maximum use of communication means other than radio.
2. Maintenance of strict circuit discipline.
3. Use of the broadcast method where possible.
4. Rotation of call signs and address groups.
5. Reduction of use of service messages.
6. Use of codress messages.
7. Encryption of all classified messages.
8. Reduction of test transmissions to minimum.
9. Avoidance of use of external routing instructions.

RADIOTELEPHONE SECURITY

Radiotelephone nets are operated so frequently that many operators tend to be careless. There are too many instances of interception of VHF/UHF transmissions at distances of many thousands of miles for this condition to continue. A large percentage of those using radiotelephone nets are officers, and the problems in formal training for educating the operators may be difficult. Certain rules apply, and all persons

having occasion to use a radiotelephone should be thoroughly familiar with them. They are:

1. Use each circuit for its intended purpose only. Keep the number of transmissions to a minimum.

2. Think out contents and wording before starting the transmission in order to reveal no information of military value, even by implication.

3. Write the message before transmission, if practicable.

4. Keep all transmissions brief, concise, and clear.

5. Transmit no classified information in plain language, including plain language references to classified titles, units, places, chart references, or persons that may reveal the nature of the headquarters, task force, or other unit concerned.

6. Avoid linkage between radiotelephone call signs and any other call signs.

7. Follow prescribed radiotelephone procedure outlined in chapter 9 of this text.

CIRCUIT DISCIPLINE AND OPERATOR TRAINING

Two basic elements in improving transmission security are circuit discipline and operator training. The communication officer is responsible for both elements.

Radio operators must adhere to prescribed circuit procedures. The importance of this is emphasized because radio is inherently the least secure means for transmitting messages. No variations, elaborations, or shortcuts in prescribed procedures are acceptable. Even individual operators are recognizable by skilled radiomen. Training should be such as to produce anonymity.

The following practices that endanger communication security are to be avoided:

1. Linkage or compromise of encrypted call signs and address groups by association with their unencrypted versions. Example: Use of unencrypted call signs in the callup, and encrypted call signs in the message heading.

2. Misuse and confusion of call signs, routing indicators, address indicating groups, and address groups by association with other call signs, routing indicators, address indicating groups, and address groups. This could result in the nondelivery of an important message, a compromise, or the linking of classified and unclassified call signs and address groups.

3. Violation of radio silence.

4. Unofficial conversation between operators.

5. Transmission in a directed net without permission.

6. Excessive repetition of prosigns or operating signals.

7. Individual mannerisms in transmitting.

8. Use of plain language in place of applicable prosigns or operating signals.

9. Use of unauthorized prosigns.

10. Unnecessary transmissions.

11. Identification of unit locations.

12. Identification of individuals belonging to an organization.

13. Excessively long calls. A unit may fail to answer, when called, owing to a condition of radio silence. Put the message on a fleet broadcast or transmit to any available station, using indefinite call signs, if necessary, instead of continuing to call. Blind transmissions are sometimes useful.

14. Failure to stand prescribed radio watches.

15. Transmitting at speeds faster than the receiving operator's ability to copy.

16. Use of excessive transmitting power.

17. Tuning transmitters with antennas cut in.

18. Excessive waste of time tuning, testing, shifting frequencies, or adjusting equipment. Drill radiomen to use their equipment properly.

19. Operating equipment off frequency. This practice can cause excessive repetition or even failure to establish communication, and increases the enemy's chances of interception and direction finding. Operate transmitters within allowed tolerances and check guard receivers on frequency at least once an hour.

CONTROL OFFICERS

In order that classified information may be controlled with maximum efficiency, the commanding officer or officer in charge of each command designates an officer to act as the classified material control officer. In commands that initiate, receive, or process Top Secret documents, he appoints a TOPSEC control officer. When an activity possesses cryptomaterial, he designates a cryptosecurity officer. Any of the designees may be the communication officer or one of his assistants.

CLASSIFIED MATERIAL CONTROL OFFICER

The classified material control officer performs the following duties:

1. Serves as the commanding officer's adviser and direct representative in cases pertaining to security of classified material.
2. Assures that all persons who are to handle classified information are properly cleared and instructed.
3. Formulates and coordinates security control measures within the command.
4. Maintains a program of declassification and downgrading of information.
5. Prepares classification guides to aid in the proper classification of material originated within the command. Preparation of such guides usually is limited to shore activities.
6. Exercises security control over visits to and from the command.
7. Reviews proposed press releases and indicates classified information that must be deleted therefrom.
8. Performs the duties of Top Secret control officer if another officer is not so designated.

TOP SECRET CONTROL OFFICER

The Top Secret control officer, subordinate to the classified material control officer, is responsible for the receipt, custody, accountability, and distribution of Top Secret information within the command and its transmission outside the command. In the performance of his duties, the TOPSEC control officer is governed by the following basic rules:

1. Avoid unnecessary dissemination of information.
2. Release to a subordinate echelon only the absolute minimum of Top Secret information necessary for proper planning or action.
3. Transmit Top Secret information within the command by direct personal contact.
4. Maintain a continuous chain of receipts for Top Secret material.

CRYPTOSECURITY OFFICER

The cryptosecurity officer is responsible for the accurate, secure, and efficient operation of the cryptocenter. Following are his more important duties:

1. Provide for and supervise the training of all crypto personnel. Recommend cryptographers for qualification by the commanding officer.
2. Ensure that all suspected compromises or violations of security are reported promptly. Great danger to the safety of the Nation can result from failure to report a compromise.
3. Ensure that a qualified cryptographer is available at all times to encrypt and decrypt messages.
4. Request message drafters to make changes as necessary to prevent errors of classification and precedence.
5. Supervise cryptographers in the performance of their duties.
6. In the event a cryptosystem is declared compromised, determine those messages originated and encrypted locally in that system, and report their contents to the commanding officer. The latter then reports to his immediate superior any compromise of significant importance.

CRYPTOGRAPHIC SECURITY

Cryptography is the science of cloaking information in codes and ciphers. A code is a system in which arbitrary groups of symbols represent units of plain text of varying length, usually syllables, words, phrases, and sentences. A cipher is a system in which individual letters of a message are replaced, letter for letter, by other letters instead of by complete words, phrases, or numbers. Cipher texts usually are transmitted in five-letter groups.

The enemy is constantly and painstakingly studying our codes and ciphers in an attempt to discover the keys to our cryptographic systems. The technique is known as cryptanalysis. The best defense against this type of enemy intelligence is cryptosecurity—the careful use of technically sound cryptosystems.

The cryptographers, under the direction of the communication officer, are responsible for the proper encryption and decryption of messages. Reliable enlisted personnel may be appointed to this board, along with officers. All cryptographers must be proficient in the use of all codes and ciphers held by the command.

Loss of a cryptographic publication or the transmission of faultily encrypted messages endangers the security of the cryptosystem. Such occurrences may require the immediate replacement of the key list, because subsequent transmissions with the same key list are considered little better than plain language. The inconvenience and expense of superseding a key list are insignificant compared to the consequences of a crypto compromise.

In all commands that hold cryptomaterial, the commanding officer, executive officer, communication officer, cryptosecurity officer, RPS custodian, and RPS custodian witnessing officers must hold Top Secret clearances. Other personnel must be cleared for access to the highest classification of cryptomaterial to which their duties require access.

Commanding officers are authorized, ex officio, access to all cryptomaterial they hold, and are responsible for authorizing access to cryptomaterial to properly cleared personnel in their commands. These personnel include on-line and off-line operators, maintenance and repair personnel, and individuals not primarily connected with operating crypto equipment but who may require access to cryptomaterials during the discharge of their duties. The commanding officer's authorization is always in writing, utilizing the letter format stipulated in NWP 16(A).

The cryptocenter is a classified communication space. For this reason, access to the space is strictly controlled. As pointed out in chapter 3, there is a single entrance with an authorized entry list posted nearby.

ON-LINE CRYPTOGRAPHIC INSTALLATIONS

In recent years the Navy has developed what is called on-line communications. This refers to communication processing systems that electronically encipher or decipher messages transmitted by teletypewriter. The older (but not obsolescent) process of enciphering or deciphering accomplished manually by members of the cryptoboard, is now referred to as off-line communications.

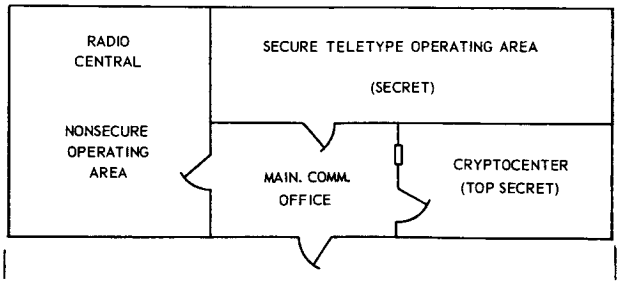
We are not concerned here with the types of on-line equipment or operating methods. The point to bear in mind is that, although on-line cryptographic procedures protect classified information during its transmission, a security problem is introduced into the communication spaces where the information is processed, because it is processed automatically into plain language. This means that anyone authorized entry into communication spaces containing on-line equipment must be cleared to handly the highest classification of material they may be received or transmitted by the equipment.

Communication spaces containing on-line equipment are divided physically into three separate areas of systems—nonsecure, secure Secret, and secure Top Secret—as in figure 10-4. Because of space limitations, the Top Secret area usually is combined with the already existing cryptocenter. On a small ship, the layout might dictate the inclusion of both the nonsecure and secure Secret areas within radio central, perhaps separated by curtains, cabinets, or merely distance. In any event, access to all the communication spaces is controlled by the CWO or, on small ships, by the operator on watch.

In the nonsecure area are the usual transmitters, receivers, and so on. Information processed in this area is vulnerable to intercept, hence classified information must be encrypted in the off-line cryptocenter. Operating personnel normally require a Confidential clearance except for those who operate off-line cryptosystems.

In the secure Secret area, information classified Secret and below normally is processed for transmission without prior off-line encryption. Personnel require a Secret clearance, with Top Secret required for those working in the cryptocenter.

On-line Top Secret circuits are limited to tactical or operational use where speed is of the utmost importance. Off-line encryption or decryption of Top Secret material, therefore, is affected only slightly by the new procedures.



105.10

Figure 10-4.—On-line communication operating spaces.

PERSONNEL SECURITY CLEARANCES

Personnel authorized access to classified information must be of—

1. Unquestionable loyalty, integrity, and trustworthiness; and
2. Excellent character and of such habits and associations as to cast no doubt upon their discretion or good judgment in handling classified information.

TYPES OF INVESTIGATIONS

The two types of personnel security investigations are the national agency check (NAC) and the background investigation (BI).

A national agency check consists of the investigation of records and files of the following agencies, as appropriate:

1. Federal Bureau of Investigation;
2. Office of Naval Intelligence;
3. Assistant Chief of Staff, Intelligence, Department of the Army;
4. Office of Special Investigations, Inspector General, U. S. Air Force;
5. Civil Service Commission;
6. Immigration and Naturalization Service;
7. Central Index Personnel and Facility Security File;
8. Bureau of Naval Personnel;
9. Headquarters, U. S. Marine Corps; and
10. Other agencies as determined by the Chief of Naval Operations (Director of Naval Intelligence).

The background investigation, much more extensive than a national agency check, develops information regarding whether access to classified information by the person being investigated is clearly consistent with the interest of national security. It inquires into the loyalty, integrity, and reputation of the individual. The BI consists of the following elements:

1. National agency check.
2. Verification of birth records.
3. Verification of last school or college attended, checking school records, and interviewing people who knew the individual while at school.
4. Examination of records of present and past employment to determine periods of service and efficiency records. Fellow employees are interviewed to determine character and reputation.
5. An interview of the majority of individual's references plus others who have knowledge of subject's background and activities.
6. Neighborhood investigation as deemed necessary to substantiate or disprove derogatory information.
7. Criminal records, including police and law enforcement agency records in areas where individual has resided for substantial periods.
8. Length of military service and type of discharge.
9. Connections individual has had with foreigners or foreign organizations both in the United States and abroad.
10. Citizenship status.

INTERIM AND FINAL CLEARANCE

A personnel security clearance is an administrative determination that an individual is eligible, from a security standpoint, for access to classified information of the same or lower category as the clearance being granted. It is emphasized that a certificate of clearance does not in itself constitute authority for access to classified information. It is merely a determination of eligibility for access. Classified information is made available to appropriately cleared persons only when a "need to know" is established clearly.

An individual may be granted either a final or an interim clearance as follows:

1. A final clearance is granted upon completion of all the various investigative requirements for the particular degree of clearance.
2. An interim clearance is a determination of temporary eligibility for access to classified information. It is granted as the result of a lesser investigative process. It is to be granted only when the delay in waiting for completion of the investigation required for final clearance would be harmful to the national interest. All requests for necessary investigations to enable a determination of final clearance should be initiated simultaneously with the procedures to issue an interim clearance.

GRANTING AND RECORDING CLEARANCES

Security is a function of command. The various investigations are carried out by the Office

of Naval Intelligence, but the final decision to grant a clearance is made by the individual's commanding officer or immediate superior The commanding officer ensures that necessary steps are taken to initiate the request for investigation in accordance with the specific instructions contained in the Security Manual for Classified Information. When the investigation is completed to his satisfaction, he issues a certificate of clearance.

Examine the personnel record of each individual, officer and enlisted, reporting on board for duty with the communication force. If no evidence of the appropriate security clearance exists (it generally is understood, for example, that all radiomen should have a clearance no less than Secret), ensure that a request for investigation is prepared. In this connection, it is the policy of the Navy Department that individual clearances be granted as the result of previous investigations, whenever feasible.

Each clearance is indicated by a properly executed Certificate of Clearance, OpNav Form 5521-429. The original and all copies are signed by the commanding officer or his delegated representative, and the ship or station seal is affixed. The original certificate of clearance is forwarded to the Chief of Naval Personnel for inclusion in the individual's personnel record. A copy is made a permanent part of the person's on-board service record, although the individual concerned does not receive a personal copy of the clearance.

Except in the case of a clearance granted as the result of a BI or NAC, it is unnecessary to issue a certificate of clearance to handle Confidential material.

INVESTIGATION REQUIREMENTS

Certain minimum investigation requirements must be met before issuance of a certificate of clearance to handle classified information. The requirements, as they apply to military personnel, are as follows:

1. Top Secret:
   a. Final clearance:
      (1) Background investigation, or
      (2) National agency check plus continuous honorable service in the Armed Forces, or a combination of active duty and civilian employment in the Government service for 15 consecutive years (with no break greater than 6 months) immediately preceding the date of the current clearance.
   b. Interim clearance: national agency check.
2. Secret:
   a. Final clearance: national agency check.
   b. Interim clearance:
      (1) Continuous honorable active duty as a member of the Armed Forces for a minimum of 2 consecutive years immediately preceding the date of the current clearance, plus
      (2) Check of ONI case history files, and the files of the Bureau of Naval Personnel or Headquarters, USMC, as appropriate.
3. Confidential:
   a. Final clearance: no formal investigation is required if the records available to the issuing command contain no derogatory information.
   b. Interim clearance: not authorized.

Security investigations remain valid and may serve as the basis for issuance of future clearances unless—

1. Derogatory information becomes available, indicating a need for further investigation; or

2. The individual is assigned to a particularly sensitive billet requiring a greater clearance criteria than indicated by the foregoing; or

3. Continuous active service in the Armed Forces and/or civilian employment in the Government service is broken by a period longer than 6 months.