CHAPTER 3

COMMUNICATION SECURITY

The security of the United States in general, and of naval operations in particular, depends in part upon the success attained in safeguarding classified information. Every Radioman 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.

In his daily work routine the Radioman learns information of vital importance to the military and to the Nation. Most of the vast amount of intelligence carried in the messages handled by naval communications passes at some point through the hands of Radiomen--data that, 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.

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

CLASSIFICATIONS

Security is a protected condition that prevents unauthorized persons from obtaining information of military value. Such information is afforded a greater degree of protection than other material and is given a special designation: CLASSIFIED MATTER. This term includes all publications, documents, cipher keys and aids, code books, letters, and messages in the four security classifications of Top Secret, Secret, Confidential, and Confidential—Modified Handling Authorized. Following are examples and definitions of each.

TOP SECRET

The Top Secret classification is limited to defense information or material requiring the highest degree of protection. It is applied only to information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in EXCEPTIONALLY GRAVE DAMAGE to the Nation, such as —

1. A war, an armed attack against the United States or her allies, or a break in diplomatic relations that would affect the defense of the United States.

2. The unauthorized disclosure of military or defense plans, intelligence operations, or scientific or technological developments vital to the national defense.

SECRET

The Secret classification is limited to defense information or material the unauthorized disclosure of which could result in SERIOUS DAMAGE to the Nation, such as —

1. Jeopardizing the international relations of the United States.

2. Endangering the effectiveness of a program or policy of vital importance to the national defense.

3. Compromising important military or defense plans, or scientific developments important to national defense.

4. 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 DEFENSE INTERESTS of the Nation, such as —

1. Operational and battle reports that contain information of value to the enemy.
2. Intelligence reports.
3. Military radiofrequency and call sign allocations that are expecially important, or are changed frequently for security reasons.
4. Devices and material relating to communication security.
5. Information that reveals strength of our land, air, or naval forces in the United States and overseas areas, identity of composition of units, or detailed information relating to their equipment.
6. Documents and manuals containing technical information used for training, maintenance, and inspection of classified munitions of war.
7. Operational and tactical doctrine.
8. Research, development, production, and procurement of munitions of war.
9. Mobilization plans.
10. Personnel security investigations and other investigations, such as courts of inquiry, which require protection against unauthorized disclosure.
11. Matters and documents of a personal or disciplinary nature, which, if disclosed, could be prejudicial to the discipline and morale of the armed forces.
12. Documents used in connection with procurement, selection, or promotion of military personnel, the disclosure of which could violate the integrity of the competitive system.

NOTE: Official information of the type described in paragraphs 10, 11, and 12 is classified Confidential only if its unauthorized disclosure could be prejudicial to the defense interests of the Nation. If such information does not relate strictly to defense, it must be safeguarded by other means than the Confidential classification.

CONFMOD

The Confidential classification has a subdivision: Confidential—Modified Handling Authorized (CONFMOD). CONFMOD may be authorized for matter the originator believes will be protected sufficiently by somewhat less strict stowage and transmission safeguards than are necessary for Confidential. CONFMOD material normally is stowed in the same manner as other Confidential material.

Material that may be classified CONFMOD includes, but is not limited to, the following:

1. Training manuals, field and technical manuals, and related materials.
2. Photographs, negatives, photostats, diagrams, and the like.
3. Defense procurement plans, including procurement contracts and related matters.
4. Communication materials, publications, and messages.
5. Charts and maps.
6. Information received from or furnished to foreign nations under international exchange of information agreements and policies.

CLEARANCES

No one may have access to classified matter without proper clearance. A security clearance is an administrative determination that an individual is eligible, from a security standpoint, for access to classified matter. If your duties require you to use classified publications and documents (and they are virtually sure to), the commanding officer is authorized to grant you clearance up to Confidential after ascertaining that you are trustworthy, discreet, and of unquestionable loyalty. Clearance to handle Secret material can be granted only after an additional check of BuPers records and an investigation by the Office of Naval Intelligence. Notation of a man's clearance is made in his service record.

COMPROMISE

No one in the Navy is authorized to handle any classified material except that required in the performance of duty. All other persons are unauthorized, regardless of rank, duties, or clearance.

If it is known—or even suspected—that classified material is lost, or passed into the hands of some unauthorized person, the matter is said to be compromised. The seriousness of the compromise depends on the nature of the material and the extent to which the unauthorized person may divulge or make use of what he learns. Never fail to report a compromise that comes to your attention.

SECURITY AREAS

The shipboard and shore station spaces that contain classified matter are known as security areas. These security areas (sometimes called 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: exclusion, limited, and controlled areas.

EXCLUSION AREA

The cryptocenter, RPIO vault, classified conference room, and other 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.

Exclusion areas are fully enclosed by walls or bulkheads 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, after being positively identified.

LIMITED AREA

Radio central, the message center, relay station, transmitter rooms, and other communication spaces usually are designated limited areas.

Operating and maintenance personnel whose duties require freedom of movement within limited areas must have proper security clearances. The commanding officer may, however, authorize entrance of persons who do not have clearances. In such instances, escorts or attendants and other security precautions must be used to prevent access to the classified information located within the area.

The entrances and exits of limited areas are either guarded or controlled by attendants to check personnel identification, or they may be protected by automatic alarm systems.

CONTROLLED AREA

Passageways or spaces surrounding or adjacent to limited or exclusion areas are often designated controlled areas.

Although the controlled area does not contain classified information, it serves as a buffer zone of security restriction and provides greater 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.

COMMUNICATION SECURITY PHASES

Communication security (COMSEC) is the protection resulting from all measures designed to deny to unauthorized persons any information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study. There are four phases of communication security: physical security, cryptosecurity, transmission security, and censorship.

PHYSICAL SECURITY

The physical security of classified material depends upon proper handling on the part of every user, proper stowage when it is not in use, and complete destruction when necessary.

Handling Precautions

Each individual in the communication organization must take every precaution to prevent intentional or casual access to classified information by unauthorized persons. When classified publications are removed from stowage for working purposes, they must be placed face down or covered when not in use. Unauthorized visitors must not be permitted in communication spaces. Never discuss classified information over the telephone. Rough drafts, carbon paper, worksheets, and similar items containing classified information should be destroyed after they serve their purpose. Meantime, they must be handled and safeguarded as classified matter.

At the close of each watch or working day, make certain that all classified material that must be passed from watch to watch is inventoried properly and that custody is transferred to your relief. All other classified matter must be locked up. Notes regarding classified matter must not be left on memorandum pads or under desk blotters. Wastebaskets should be checked to see that they contain no classified material such as notes, carbon paper, excess copies, or rough drafts. These items must be placed in burn bags with other classified material and the burn bags properly stowed until destroyed according to a schedule promulgated by the communication officer or custodian.

Vaults, safes, or lockers used for stowage of classified matter must always be kept locked when not under the supervision of authorized personnel. Cryptographic aids and related classified matter must never be left unguarded by the user. You should habitually rotate the dial of all combination locks at least three complete turns in the same direction when securing safes, files, and cabinets. In most locks, if the dials aregiven only a quick twist, it is possible sometimes to open the lock merely by turning the dial in the opposite direction. Always assure yourself that all drawers of safes and file cabinets are held firmly in the locked position.

If you are working with classified material and are interrupted by a fir alarm or other emergency, which requires you to leave the classified material unguarded, it should be stowed in the same manner as at the end of a working day. It is your personal responsibility to safeguard all classified material in your possession.

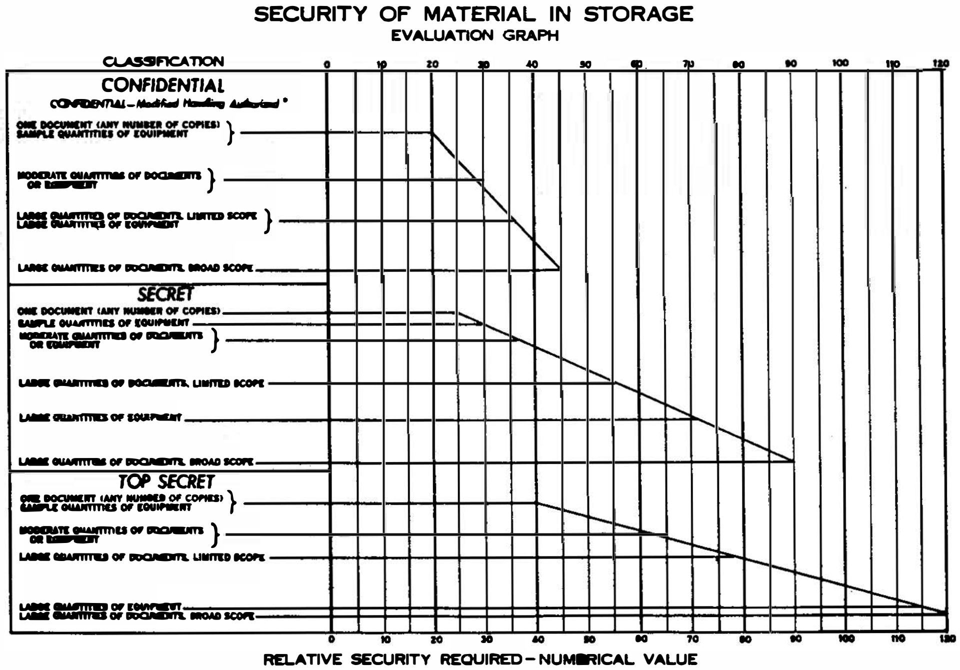
Stowage

All classified matter not in actual use must be stowed in a manner that will guarantee its protection. The degree of protection necessary depends on the classification, quantity, and scope of the material.

A numerical evaluation system has been developed for determining the relationship between the security interest and the level of protection required. The more secure the stowage facilities, the higher the numerical values assigned.

The graph, figure 3-1, shows the numerical values required for quantity and type of documents of each classification. The table, figure 3-2, is a guide for evaluating stowage facilities. These two must be used together.

For example, a ship stows plain language translations of encrypted messages in a heavy steel safe in the cryptocenter. Visitors are not allowed in any of the communication spaces, and only cryptographers may enter the cryptocenter itself or remove anything from its safe. The cryptographer on watch acts as a guard in attendance at the container. From the table (fig. 3-2), we can assign a numerical value to these facilities as follows:



Documents and material designated Confidential-Modified Handling Authorized will normally be stored in the same manner as other Confidential material. When this is not feasible, such documents and material will be stored in a container equipped with a reasonable secure locking device or in any other manner determined by competent authority which will afford adequate protection. This does not preclude a more secure means of storage if desired.

31.2

Figure 3-1.—Numerical values required for quantity and type of documents of each classification.

1. SHELTER	VALUE
None	0
Light structure, such as a quonset hut, which can be locked and barred	10
Heavy structure, such as masonry building	15
Commissioned ship	15
2. STOWAGE CONTAINER	
None	0
Any portable container	0
Wooden container, any type of lock	2
Metal container, key lock	5
Metal container, combination lock	15
Lightweight steel safe	20
Light vault	20
Heavy steel safe	30
Bank vault	40
3. GUARDING	
Unguarded	0
Military guard in general area	15
Military guard checks container every hour	20
Military guard checks container every 30 minutes	25
Military guard in attendance at container	35
No supporting guard force	0
Military supporting guard force	20
4. PROTECTIVE ALARM SYSTEM	
No alarm on container	0
System to detect opening of container	15
System to detect tampering with or opening of container	20
System to detect approach to, tampering with, or opening of container	30
No general area alarm	0
System to detect entry into general area	25
5. CONTROL OF PERSONNEL ACCESS TO CONTAINER WHEN CLOSED, AND TO CONTENTS WHEN OPEN	
System necessary but not in effect	-20
System not required	0
System in effect	5

41.1

Figure 3-2.—Table of numerical equivalents (simplified).

	Value
Sheltered aboard a commissioned ship	15
Stowed in heavy steel safe	30
Military guard in attendance at container	35
System in effect for control of personnel access to container when closed, and to contents when open	5
TOTAL	85

From the graph (fig. 3-1) you can see that stowage facilities with a numerical value of 85 are secure enough for everything but the most sensitive class of Secret and the two most sensitive classes of Top Secret material.

The keys or combinations to safes and lockers containing classified material are made available only to persons whose duties require access to them. The keys or combinations must be changed at least every 6 months. They also must be changed whenever any person having knowledge of them is transferred from the organization, and at any time the keys or combinations are suspected of being compromised.

Any time you find a safe or cabinet containing classified material unlocked and unattended by assigned persons, be sure to report the condition immediately to the senior duty officer. Do not touch the container or contents, but guard them until the duty officer arrives. The duty officer then assumes responsibility for such further actions as locking the safe, recalling the responsible persons, and reporting the security violation to the commanding officer.

Consult chapter 6 of the Department of the Navy Security Manual for Classified Information for further details on stowage of classified matter.

Destruction

The destruction of classified matter falls into two categories: routine and emergency. Destruction, when authorized or ordered, must be complete.

ROUTINE DESTRUCTION. — The destruction of superseded and obsolete classified materials that have served their purpose is termed routine destruction. Routine destruction of publications, message files, and certain cryptomaterials is carried out when authorized by specific directives. These directives are found in the letter of promulgation of the publication itself, in cryptographic instructions and manuals, and in U. S. Naval Communication Instructions (DNC 5 series). Other materials, such as classified rough drafts, worksheets, and similar items, are destroyed, as necessary, to prevent their excessive accumulation.

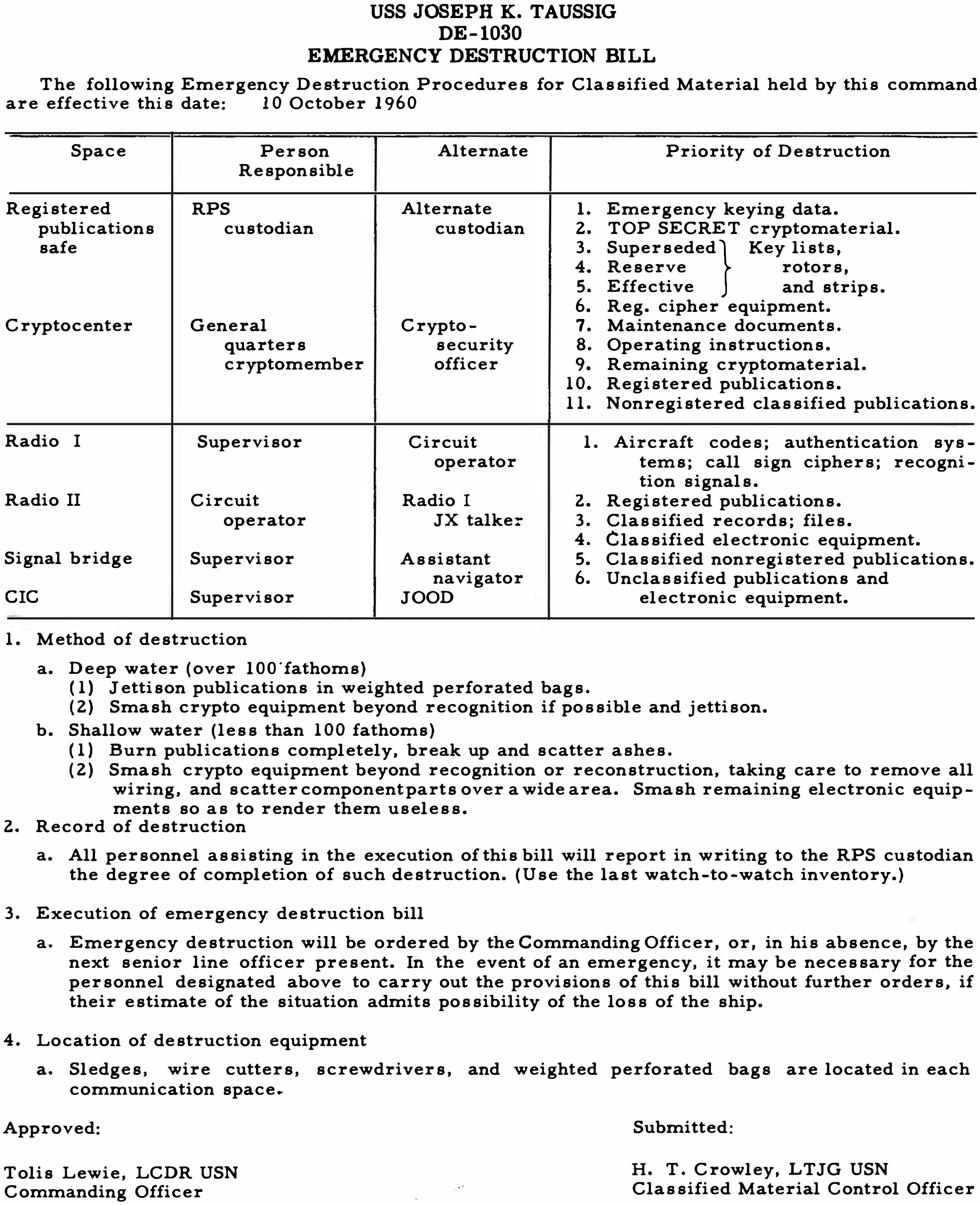
The most efficient method of destroying combustible material is by burning. It is likely, therefore, that you will be called upon to assist in burning classified material. As a member of the burn detail, you should know exactly what is to be burned and should doublecheck each item before it is burned. To facilitate complete destruction of bound publications, tear them apart, crumple the pages, and feed the pages to the fire a few at a time. If burn material is carried in a bag that is not to be burned, turn the bag inside out to make certain every piece of paper is removed and burned. The material must be watched until it is completely consumed, and ashes broken up and scattered so that no scraps escape destruction.

When no incinerator is available, which often is true aboard ship, classified material may be burned in a perforated metal drum or container with a cover of wire netting.

EMERGENCY DESTRUCTION. — Emergency destruction of classified material is authorized at any time when necessary to prevent its capture by an enemy. On board ship, classified material is not subjected to the same risks as on land. However, if a ship is in danger of sinking or is severely disabled, action is taken in accordance with the ship's emergency destruction bill (fig. 3-3), the execution of which is an all-hands evolution from communication officer to striker. This bill details the method and the order of destruction of classified matter. Each man in the communication division is assigned responsibilities by duty and watch instead of by name. The bill provides alternates for each billet to ensure effective action despite personnel casualties.

Destruction plans call for the highest degree of individual initiative in preparing for and in actually commencing the required destruction. It is extremely important for all Radiomen to understand that, in emergencies subjecting classified material to compromise through capture, they must start necessary destruction under the plan without waiting for specific orders.

Cryptographic material has the highest priority for emergency destruction. Insofar as humanly possible, it must not be permitted to fall into enemy hands. After cryptomaterial is destroyed, other classified communication



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 1960

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.
Cryptocenter	General quarters cryptomember	Crypto-security officer	7. Maintenance documents. 8. Operating instructions. 9. Remaining cryptomaterial. 10. Registered publications. 11. Nonregistered classified publications.
Radio I	Supervisor	Circuit operator	1. Aircraft codes; authentication systems; call sign ciphers; recognition signals.
Radio II	Circuit operator	Radio I JX talker	2. Registered publications. 3. Classified records; files. 4. Classified electronic equipment.
Signal bridge	Supervisor	Assistant navigator	5. Classified nonregistered publications. 6. Unclassified publications and electronic equipment.
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

76.7

Figure 3-3.— Emergency destruction bill (typical).

material is destroyed in the order of classification—highest classified material first. Next in importance in the destruction plan is classified (noncryptographic) communication equipment, followed (if time permits) by destruction of unclassified material and equipment.

Destruction by fire is the preferred method for all combustible materials. Oil or chemicals may be used to facilitate burning. If the ship is in deep water, and time does not permit burning classified publications, messages, files, and logs, they may be placed in weighted perforated canvas bags and thrown overboard (jettisoned). Classified equipment may also be jettisoned in water deep enough to preclude any possibility of recovery. Water over 100 fathoms is usually considered deep enough to prevent the enemy from conducting successful salvage operations.

If the ship is in shallow water (100 fathoms or less), combustible classified material must be burned, and may be jettisoned only as a last resort. Classified communication equipment must be smashed beyond recognition before jettisoning in shallow water, and unclassified communication equipment should be demolished beyond repair.

A sufficient number of perforated canvas bags and tools, including sledge hammers, screwdrivers, and wire cutters, are always kept in communication spaces for use in emergency destruction.

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 complete words, phrases, or numbers. Cipher texts usually are transmitted in 5-letter groups.

The cryptoboard, under the direction of the communication officer, is responsible for the proper encryption and decryption of messages. Along with officers, reliable enlisted personnel may be appointed to this board. Members of the board, known as 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 frequently require the immediate replacement of the key list used, for subsequent transmissions with the same key list might be little better than plain language. The work and expense of superseding a key list, though great, are insignificant compared with the consequences of compromise.

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

TRANSMISSION SECURITY

Transmission security is that component of communication security which results from all measures designed to protect transmissions from unauthorized interceptions, traffic analysis, and imitative deception.

Some methods of transmission are more secure than others. In general, the means and types of transmission, in their order of security, are as follows:

1. Messenger;
2. Registered mail (guard mail, U. S. postal system, or diplomatic pouch);
3. Approved wire circuits;
4. Ordinary mail;
5. Nonapproved wire circuits;
6. Visual (semaphore, flaghoist, flashing light);
7. Sound systems (whistles, sirens, bells);
8. Radio

Messenger

Classified matter is transmitted by messenger when security—not speed—is the paramount objective. The principal messenger agency for the Department of Defense is the Armed Forces Courier Service (ARFCOS). This agency is responsible for the safe transmittal of highly classified matter to military addressees and certain civilian agencies throughout the world. ARFCOS courier transfer stations are located in designated areas. Every item of classified material sent via ARFCOS is in the physical custody and control of a commissioned officer courier from the time of entry into the system until the addressee or his authorized representative receipts for it. Classified material that may go by registered United States mail is not transmitted by AFRCOS.

Guardmail is another type of messenger service for transmitting classified material, although unclassified material is also delivered by this means. Reliable petty officers as well as commissioned officers are appointed as guard mail messengers. Guard mail is used, for instance, in a naval district for delivering mail to other military or Government activities located in the same area, and also in conjunction with ordinary mail service to and from ships in port.

Mail

In addition to transmitting unclassified material, the United States postal system is used to transmit classified material except Top Secret matter and cryptographic aids and devices. Secret and Confidential matter must be sent by registered mail instead of by ordinary mail, and must not enter a foreign postal system. The single exception to this is that material addressed to Canadian Government activities is permitted to pass through the Canadian postal system. Material classified CONFMOD may be sent by ordinary first class mail through both United States and Canadian postal systems. The great bulk of the Navy's administrative traffic is sent by mail, thus reserving radio circuits for operational traffic insofar as possible.

Mailable Secret and Confidential matter is double-wrapped, as shown in figure 3-4. Top Secret matter is prepared similarly, but does not, of course, go through the mails. Use of the inner envelope is not required for CONFMOD material.

Wire Circuits

When available, wire circuits invariably are used in preference to radio, because they are less susceptible to interception.

Wire systems are of two types: approved and nonapproved.

An approved circuit is one designated by proper authority for the transmission of classified information in the clear. Messages classified Secret and below may be transmitted on such circuits.

A nonapproved circuit is one that is not designated by proper authority for the transmission of classified information in the clear.

Telephone circuits normally are considered nonapproved and are not used to discuss classified data unless specifically designated as approved. Approved telephone circuits are equipped with security devices to minimize the possibility of wire tapping.

Tapping often may be discovered by physical examination or by transmission irregularities. Interception by induction, however, can escape detection completely. Supersensitive devices placed near the wire circuit pick up sounds through a 2-foot wall. Tiny microphones, hidden in telephone receivers, pick up not only telephone conversations but voices anywhere in the room.

Underwater cables also are liable to unauthorized interception, although they are more difficult to tap than landlines. Submarines are able to make successful interceptions through induction. The point where the cable emerges into shallow water is the most vulnerable.

Visual Communications

Visual communication systems are used in preference to radio except at night when there is a possibility of divulging the ship's position. They are more secure than radio because reception is limited to units in the immediate vicinity of the sender.

Visual communication methods rank, in order of security, according to the distance from which the signals can be seen. In daylight the relative order is semaphore, directional flashing light, panels, flaghoist, pyrotechnics, and nondirectional flashing light. At night the order is infrared, directional flashing light, pyrotechnics, and nondirectional flashing light.

The greatest care must be taken to ensure that signal lights are used only when necessary, and that the minimum of light is employed. An exception is for recognition signals, which must be sent on a light sufficiently brilliant to be seen at once.

Transmission of plain language message is kept to a minimum. This is because many persons are adept at reading lights and flags.

Sound Systems

Whistles, sirens, foghorns, bells, and underwater sound devices are common types of sound systems. They are utilized by vessels to transmit emergency warning signals (air raid alerts, mine sighting, etc.) and for signals

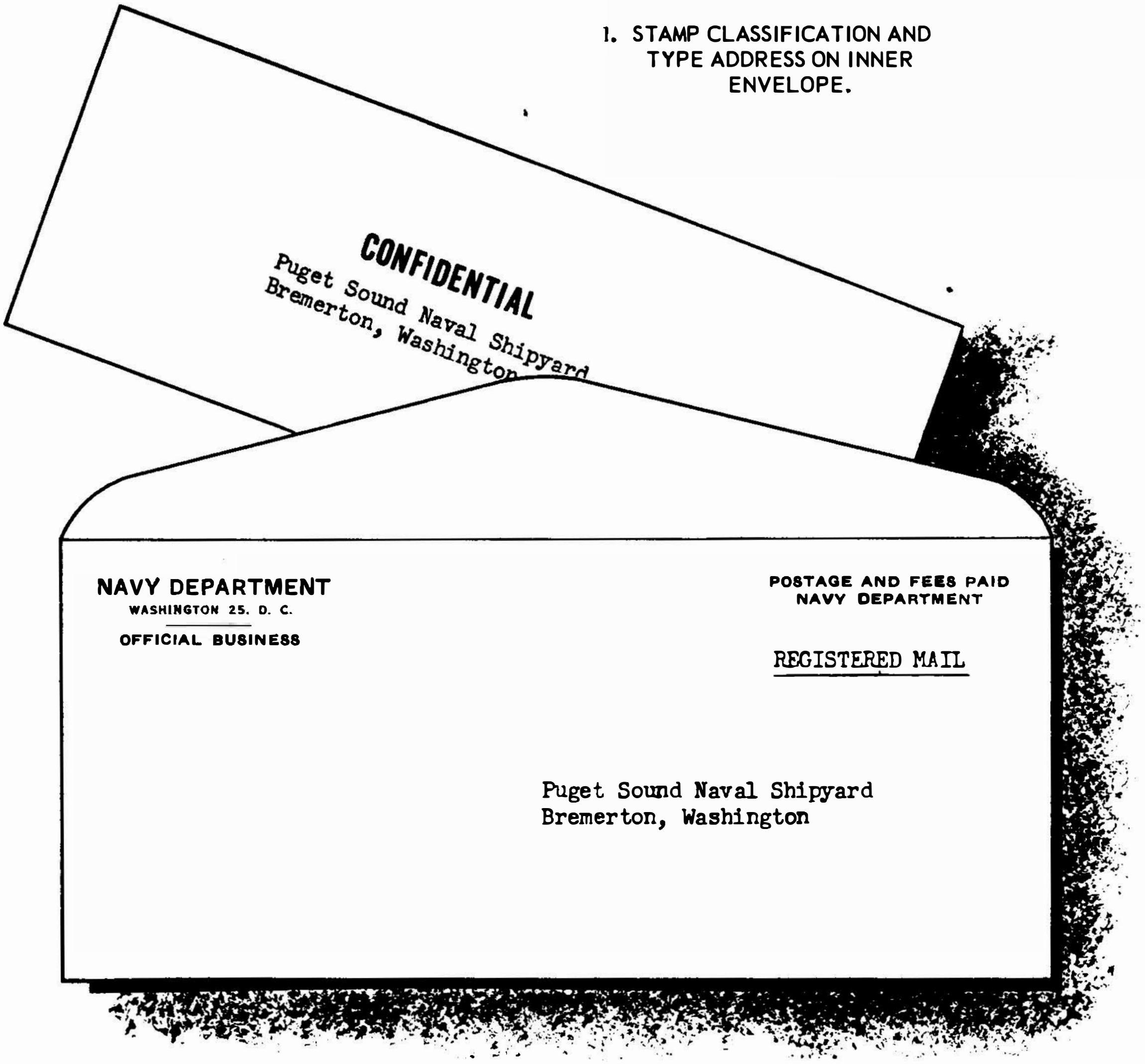

1. STAMP CLASSIFICATION AND TYPE ADDRESS ON INNER ENVELOPE.
CONFIDENTIAL
Puget Sound Naval Shipyard
Bremerton, Washington
NAVY DEPARTMENT
WASHINGTON 25. D. C.
OFFICIAL BUSINESS
POSTAGE AND FEES PAID
NAVY DEPARTMENT
REGISTERED MAIL
Puget Sound Naval Shipyard
Bremerton, Washington
2. ADDRESS A LARGER ENVELOPE INTO WHICH THE SMALLER ONE CAN BE INSERTED. DO NOT SHOW CLASSIFICATION ON OUTER ENVELOPE.

Figure 3-4.—How mailable classified matter is prepared. 6.1

prescribed by the Rules of the Road. Sound systems have the same range limitations as visual methods and are less secure. Their use is largely restricted to maneuvering and emergency situations.

Radio

Radio is potentially the least secure means of communication. A message sent by radio is open to interception by anyone who has the necessary equipment and is within reception range. Thus, in addition to obtaining intelligence, the enemy may be able to fix the location of operating forces through direction finding. By employing deceptive techniques, he could confuse and hamper our communications and, by traffic analysis, forecast the intentions of our forces.

Uses of radio in the ultrahigh frequency (UHF), superhigh frequency (SHF), and extremely high frequency (EHF) ranges normally have security approaching visual means. Experience has proven, however, that transmissions of these frequencies beyond line-of-sight distances are frequently exceeded. Consequently, it is important that all users recognize the possibility of interception at distances far beyond the normal usable ranges.

Despite its shortcomings, though, radio still is the primary means of communication. It is fast, reliable, and often the only method of maintaining contact between distant and highly mobile units. A satisfactory degree of security can be obtained only by its proper and intelligent use.

INTERCEPT AND DIRECTION FINDING. — The best defense against enemy intelligence efforts by interception and direction finding is strict radio silence. It is apparent that the enemy cannot gain intelligence from radio transmissions if none are sent. Radio silence is placed in effect when it is reasonable to assume that the enemy is unaware of the location or impending movements of a ship or force. If it is impracticable to maintain radio silence, the following defensive measures make interception and direction finding more difficult:

1. Avoid unauthorized transmissions and unnecessary testing.
2. Use combinations of transmitters, antennas, and power to produce minimum wave propagation and emission intensity consistent with reliable communications.
3. Use the broadcast method of transmitting traffic in preference to the receipt method.
4. Conceal instructions to shift frequency by using an encrypted message in the absence of a prearranged plan.
5. Adjust transmitters accurately and adhere to frequency tolerances, thereby preventing the need for repeating messages or parts of messages.
6. Maintain strict circuit discipline.

TRAFFIC ANALYSIS. — The enemy may gain valuable information from his study of our communications by traffic analysis. Traffic analysis includes the study of message headings, receipts, acknowledgments, relays, routing instructions, and service messages; tabulating the volume, types, and directional flow at each point; and correlating information taken from unclassified messages, noting departures from normality.

Assume that within a short time a radio message is transmitted from point Bravo to Romeo, another to Victor, another to a unit of the fleet operating off Whiskey, and a fourth to a unit off Oscar. The enemy's traffic records show that messages rarely are transmitted to these four addressees simultaneously. They also reveal that previous transmissions of this type were followed by arrival of a convoy at point Romeo. The enemy may logically conclude that a convoy from Bravo to Romeo is planned, and that these transmissions probably are arranging for an escort.

Some measure that can be taken to render traffic analysis by the enemy more difficult and less reliable include —

1. Minimum use of radio.
2. Maintenance of strict circuit discipline.
3. Rotation of frequencies.
4. Rotation of call signs and address groups for encryption.
5. Minimum use of service messages, correction requests, and repetitions.
6. Concealment of originator and addressees in the text of an encrypted message.
7. Avoidance of long, easily associated messages of a recurrent nature.
8. Control of the timing and volume of test transmissions to avoid revealing information about pending operations.
9. Keeping external routing instructions to a minimum.
10. Use of Encrypt for Transmission Only (EFTO) procedure. (See OpNav Instruction 2220.3 for complete details.)

IMITATIVE DECEPTION. — An enemy may attempt to enter communication nets used by the Navy in order to confuse and deceive our forces. This practice is known as imitative deception. There are many deceptive techniques the enemy might use to obstruct our radio communications. He may, for example —

1. Remove a message from one circuit and introduce it on another circuit to waste time, create confusion, and produce service messages.
2. Intentionally garble the text of a genuine message and combine it with the heading of another, then introduce it on a different radio net.
3. Originate and transmit false plain language messages.
4. Call a unit in the hope of taking bearings on the answering transmission.
5. Partly obliterate a false message to conceal lack of knowledge of authenticators or call signs.

The best defense against imitative deception is proper authentication. This is a security measure to protect communication systems against fraudulent transmissions. An authenticator is a group of characters (usually two randomly selected letters) inserted in a message to prove its authenticity. Any authentication system has accompanying instructions specifying the method of use and transmission procedures. By its correct use, the operator can distinguish between genuine and fraudulent stations or transmissions. A station may include authentication in a transmitted message—called transmission authentication. Another use is known as challenge and reply authentication. In this method the sending station transmits a challenge from which the receiving operator must ascertain the correct reply authenticator. The challenging station must determine the reply to be correct before any exchange of messages commences. Authentication is mandatory when —

1. Any station suspects imitative deception on a circuit.
2. Any station is challenged or requested to authenticate.
3. Making contact and amplifying reports in plain language or brevity code.
4. Directing radio silence or requiring a station to break an imposed radio silence.
5. Transmitting a plain language cancellation of an encrypted message by radio or by other methods when sending stations cannot be recognized.
6. Transmitting to a station that is under radio silence.

Authentication is advisable under the following circumstances:

1. When transmitting operating instructions affecting the military situation; for example, closing down a station or shifting frequency.
2. When making initial radio contact. Authenticators should be exchanged to prevent an enemy station from opening a circuit by asking a legitimate station to authenticate.

Good judgment sometimes dictates that an operator accept a message instead of arguing over authentication, even though he may doubt its genuineness. Such a message should be delivered promptly to the addressee with the operator's notation that it was not properly authenticated. The decision regarding its authenticity is made by the addressee.

Other effective defenses against imitative deception are —

1. Thorough training in operating procedures, as described in subsequent chapters.
2. Alertness of operators to recognize irregularities in procedure and the minor implausibilities that often characterize enemy deceptive efforts.
3. Direction finding on transmissions of questionable origin.
4. Minimum use of plain language and procedure messages.

Maintaining a high degree of circuit discipline on the part of operators also lessens the chances of enemy deception. Circuit discipline can be attained only through net control, monitoring, and training. It includes adherence to prescribed frequencies and operating procedure. Negligence, inaccuracy, and laxity, as well as lack of circuit discipline and operator training, are some of the common causes of violations that endanger radio transmission security. Circuit discipline is discussed in greater detail in chapter 6.

JAMMING. — Jamming is another method an enemy may use in his efforts to disrupt our communications. It is accomplished by transmitting a strong signal on the victim frequency. You must be able to recognize jamming, cope with it, and, at the same time, prevent the enemy from knowing the effectiveness of his efforts. Common forms of jamming are —

1. Several carriers adjusted to the victim frequency, each carrier modulated by an audiofrequency.
2. Simulated traffic handling on the victim frequency.
3. Random noise amplitude-modulated carriers.
4. Continuous-wave carrier (keyed or steady).
5. Several audio tones in rapid sequence, modulating a carrier (called bagpipe, from its characteristic sound).

Many measures can be used to counter and minimize the effects of jamming. Some of these measures are:

1. Route messages via alternate circuits, meanwhile continuing live traffic on the jammed circuit to create the impression that the jamming is ineffective.
2. Use different receivers to take advantage of differences in selectivity. Selectivity is the ability of a receiver to discriminate between signals close together.
3. Make maximum use of the directional effects of available antennas.
4. Request the sending station to increase power or to shift frequency.
5. Take advantage of split-phone reception by copying signals simultaneously keyed on two frequencies.

6. Keep the receiver volume at a low level when copying through jamming. Your hearing can better discriminate between signals that aren't too loud.

Each occurrence of jamming must be reported promptly to cognizant authorities. Information concerning these reports is found in NWP 33.

SECURITY OF RADIOTELEPHONE. —Radiotelephon transmissions are the least secure method of radio communication. Anyone within range, who speaks the language used, can understand the transmissions. Circuit discipline and procedure often are poor on radiotelephone circuits because the equipment can be, and often is, operated by someone besides trained radio personnel. Poor circuit discipline and improper procedure slow communications, cause confusion, and may divulge information to the enemy.

Our best defense against enemy intelligence efforts is strict adherence to prescribed radiotelephone procedures. With this in mind, here are a few precautions to observe when communicating by radiotelephone:

1. Use each circuit for its intended purpose only.

2. Keep the number of transmissions to a minimum.

3. Write the message before transmission, if possible.

4. Keep transmissions brief, concise, and clear.

5. Transmit no classified information in plain language.

6. Avoid linkage between radiotelephone call signs and other types of call signs.

Radiotelephone procedure is discussed in detail in chapter 7.

CENSORSHIP

Censorship is an essential form of protecting military information. It includes censorship of our personal communications as well as official communications. Personal censorship should be cultivated until it becomes second nature.

In the course of your duties, you may possess highly classified information, the knowledge of which is shared oftentimes only by the commanding officer, the communication officer, and yourself. You must be alert against a slip of the tongue that might reveal this information to someone not authorized to know. The Security Manual states that "indiscreet conversation and personal letters constitute the greatest menaces to security." The only safe policy to follow concerning classified information is KEEP YOUR MOUTH SHUT AND YOUR PEN DRY. When on duty, discuss classified subjects only as necessary to accomplish your job. When off duty, don't discuss classified matters with anyone. This includes your family and best friend. The desire to impress others with the importance of your job is usually quite strong. Divulging classified information is a very unwise way of trying to impress anyone, particularly when you may be endangering your country and many lives.

Loose talk in public places is even more dangerous. Conversation in restaurants, hotel lobbies, railroad stations, elevators, taverns, and other public places can be overheard easily. Foreign agents are scientifically trained to collect particles of seemingly harmless information from such conversations. Once pieced together and analyzed, they sometimes reveal military information of incalculable value.

Mail likewise is subject to interception by the enemy. The following topics must not be mentioned in personal correspondence:

1. Location, identity, or movement of ships or aircraft.

2. The forces, weapons, military installations, or plans of the United States or her allies.

3. Casualties to personnel or material by enemy action.

4. The employment of any naval or military unit of the United States or her allies.

5. Criticisms of equipment or morale of the United States or her allies.

Personal censorship also extends to telephone conversations. As we have seen, telephone wires can be tapped, and conversations can be overheard at the switchboard and other points along the circuit. Never discuss classified information over a nonapproved telephone line.

Diaries can be fruitful sources of information for the enemy. They sometimes reveal secrets the enemy laboriously is attempting to extract through cryptanalysis. Even in peacetime, lost and stolen diaries can cause serious damage to the prestige of your Nation.

CALL SIGN ENCRYPTION

Call signs and address designators are encrypted to conceal the identity of the originator and addressees of certain types of messages. The encryption and decryption of these call signs is part of your job, hence you must become proficient in using the call sign cipher device. Operating instructions for the device may be obtained from the registered publications custodian. More likely, though, your supervisor will show you how to operate the device.

An operator must exercise extreme care when transmitting a message containing encrypted call signs. From force of habit he may use the unencrypted international call sign in establishing communications and then send the encrypted version in the message. This results in a compromise of the call sign and gives enemy intelligence a lever with which he may break the entire system.

CONELRAD AND EMCON

Control of electromagnetic radiation (from which the word conelrad is derived) is the control of equipment capable of emitting radio waves to reduce the likelihood of interception by the enemy. It embraces radio communication equipment, radar, navigational aids (beacons), identification devices (IFF), and aerological devices (radiosonde).

Two terms are applicable when referring to control of electromagnetic radiation. Conelrad is used in the Department of Defense Plan within the United States and the Panama Canal Zone. The term EMCON (short for emission control) is used in the U. S. fleet.

In peacetime, conelrad or EMCON restrictions are imposed only if required for operational purposes or for training. The various degrees of restrictions are found in NWP 16(A).

SECURITY VERSUS SPEED

A variable relationship exists between security and speed in communications. In the planning stages of an operation, for example, when only a few should know what is plann d, security considerations are paramount. As the time of execution approaches, additional persons must know the plan, and preparations cannot be concealed so effectively. Then, speed is increasingly important. In actual combat, plain language transmission of classified information may be authorized, although security cannot be totally disregarded even then.

ADDITIONAL SECURITY INFORMATION

The security precautions mentioned in this manual do not guarantee protection, nor do they attempt to meet every conceivable situation. The man who adopts a commonsense outlook, however, in addition to knowledge of the basic regulations, can solve most security problems.

The effective editions of the following publications contain additional information on security. Those marked with an asterisk are classified.

Department of the Navy Security Manual for Classified Information, OpNavInst. 5510.1B

U. S. Navy Physical Security Manual, OpNavInst. 5510.45

Security, Armed Forces Censorship, OpNavInst. 5530.6

U. S. Navy Regulations, 1948, chapter 15

*RPS 4

DNC 5

*ACP 122

*NWP 16(A)

The Naval Communications Bulletin, published quarterly by DNC (with classified supplement*)

Navy directives in the 2200-2260 series (communication security) and in the 5500-5599 series (administrative security)

For information on local security rules, study the security regulations of your ship or station.