TABLE OF ARTICLES(CONTINUED)

CHAPTER FIVE

COMMUNICATION SECURITY

SECTION A

5000. PROTECTION OF COMMUNICATIONS

5001. RESPONSIBILITY OF THE COMMANDING OFFICER

.1 The commanding officer is responsible for maintaining communication security. (See Article 1301, SECURITY MANUAL.)

.2 In addition to maintenance of communication security within his own command, it is the duty of a commanding officer to report serious breaches of communication security to offending ships or stations as soon as practicable with due regard for the requirements of radio silence.

5002. COMPONENTS OF SECURITY

.1 Communication security is the protected condition of communications resulting from the application of various measures to prevent or delay an enemy from gaining military information from our communications.

.2 Communication security is a means - not an end. Rules governing communication security do not guarantee security and they do not attempt to meet every conceivable situation. Operational requirements limit the security measures that can be employed. With operational efficiency, it is possible to obtain a satisfactory degree of security with a minimum of delay or interference.

.3 Phases of communication security are as follows:

(a) Physical security. (Section B)

(b) Cryptosecurity. (Section C)

(c) Transmission security. (Section D)

(d) Censorship. (Section E)

5003. SECURITY MEASURES

.1 Security measures for cryptomaterial, messages, communication equipment and other classified communication material include defenses against the following:

(a) Capture or salvage.

(b) Theft, espionage, observation and photography.

(c) Interception.

(d) Radio direction finding.

(e) Traffic analysis.

(f) Imitative deception.

(g) Cryptoanalytic attack.

5004. SECURITY AND SPEED

.1 Reliability of communications is always paramount. However, there is a variable relationship between security and speed:

(a) In the planning stages of an operation, when only a few should know what is contemplated, security considerations are dominant.

(b) As the time of execution approaches, additional persons must know the plan, and preparations cannot be concealed so effectively. Then speed is increasingly important.

(c) In combat, plain language may be authorized but security must not be disregarded.

.2 Modern cryptosystems permit security with speed - speed with security.

5010. CLASSIFICATION OF MATTER

5011. DEFINITIONS

.1 Classified matter is information or material in any form or of any nature which, in the public interest or in the interest of the service or of persons within the service, must be safeguarded in the manner and to the extent required by its importance and by its relation to other classified information.

.2 Registered matter is classified matter to which a registered number is assigned, and which is accounted for at prescribed intervals and upon specified occasions.

5012. GRADES OF CLASSIFICATION

.1 Classified messages will be designated Top Secret, Secret, Confidential, or Confidential-Modified Handling Authorized, whenever their contents fall within the definitions set forth in Chapter 3 of the SECURITY MANUAL.

.2 Markings of classification shall be well clear of the edges so as not to become covered in assembling or trimming.

5013. PURPOSE OF CLASSIFICATION

.1 The primary purpose of classification is to impose restrictions on the handling of messages and dissemination of the information contained therein. The higher classifications lose their significance when overused. The classification of messages must receive careful consideration by the originator, since both overclassification and underclassification are to be avoided.

.2 The degree of cryptosecurity afforded a message seldom is governed by its classification.

5014. RESPONSIBILITY FOR CLASSIFICATION

.1 Officers in a command status are responsible for the classification and reclassification of matter originated within their jurisdiction. This authority may be delegated to subordinates by the officer in command status, but the delegating authority is not thereby relieved of responsibility for assignment of proper classification.

5014. (Continued)

.2 The authority to assign Top Secret classification may be delegated only to specifically designated officers or officials.

5015. DETERMINING CLASSIFICATION

.1 Matter which requires classification within the meaning of Article 5011.1 shall be assigned the lowest classification consistent with the necessary security and dissemination of such matter or information.

.2 The precautions necessary for the security of classified messages must be indicated by the assignment of a designation of Category A, Category B, or Category AC. Instructions pertaining to message category markings are found in the SECURITY MANUAL and NWIP 16-1.

5020. DISSEMINATION OF CLASSIFIED MATTER

5021. RESTRICTION OF DISSEMINATION

.1 Officers in a command status are responsible for controlling the dissemination of classified matter emanating from or distributed within their command and for promulgating additional directives as necessary to prevent unauthorized dissemination of classified matter under their control.

.2 Classified information may be divulged only to those persons whose official duties require its knowledge or possession.

.3 No person is entitled to knowledge or possession of classified matter by virtue of his rank, position, office or clearance.

.4 Only specifically designated personnel may handle and process Top Secret information.

5022. PROVISION FOR SPECIAL PRIVACY

.1 No departure from standard established classifications will be made in naval messages. Where a message of any classification has important personal implications, the originator may use an appropriate phrase to ensure special handling and specific dissemination. (See Article 7073.)

.2 Instructions for special handling of Top Secret and other messages requiring special privacy are contained in NWIP 16-1.

5023. AVAILABILITY OF CLASSIFIED INFORMATION AND PUBLICATIONS

.1 Optimum efficiency, accuracy and security require that sufficient working publications, directives, task organizations, communication plans and other classified matter relating to communications be available to operating personnel. Watch-to-watch accountability of such classified information will make it available to the necessary personnel and provide the required security.

5024. LOSS, COMPROMISE, UNAUTHORIZED DISCLOSURE

.1 Each person who has knowledge and/or custody of classified matter is responsible for any act or failure on his part which may in any way contribute to its loss, compromise or unauthorized disclosure.

.2 Unsuspected physical compromise is far more serious than outright loss. If for example an undisclosed compromise to a cryptographic system

5024.2 (Continued)

occurs and the system continues in use, the enemy may be able to read all the traffic sent in that system.

.3 Loss, compromise or unauthorized disclosure of classified matter will be handled as set forth in the following references:

(a) Registered classified matter in accordance with RPS 4.

(b) Nonregistered classified matter in accordance with Article 0801 of the SECURITY MANUAL.

.4 When, by orders of competent authority, classified matter is divulged to persons outside the Naval Establishment, such persons shall be informed in writing of the classification of the matter. When applicable, they shall be advised of their liability to prosecution under the Espionage Act or the Atomic Energy Act in the event of unauthorized disclosure.

SECTION B

5100. PHYSICAL SECURITY

5101. REPORTING IRREGULARITIES

.1 All personnel are responsible for bringing to the attention of their immediate superiors any irregularities in communications which may affect communication security.

5102. IMPORTANCE OF PHYSICAL SECURITY

.1 Maintenance of physical security assures the maximum protection of classified material from production to destruction. Classified material may be safeguarded from compromise by:

(a) Proper handling on the part of everyone concerned;

(b) Proper stowage when not in use;

(c) Complete destruction when necessary.

5103. PROTECTION OF CRYPTOSYSTEMS AND CRYPTOMATERIAL

.1 The number of cryptosystems and quantity of cryptomaterial held shall be maintained at a minimum in the following situations:

(a) At exposed outposts;

(b) In aircraft;

(c) In ships operating in water under enemy control of such depths that salvage operations are practicable;

(d) Under any other circumstances where capture is a probability.

.2 A GUIDE to assist in maintaining the proper safeguards for classified material follows:

(a) Are all personnel having access to classified material periodically warned of the danger of loose talk in public and private places?

(b) Are the combinations on safes which contain classified material changed every six months, or whenever any person having access to a safe is detached or transferred from the office?

(c) Is someone appointed to inspect each safe, desk, and file at the close of every working day to make certain that everything is stowed properly? Is a record made of each inspection?

(d) Are classified documents and material invariably locked up when not in use?

(e) Are burn bags used, and are wastebaskets checked each day to make certain that they contain no classified material, including shorthand notes, carbon paper, or rough drafts? Is classified waste material promptly and properly destroyed?

(f) Is it determined that notes regarding classified matter are not left on memorandum pages or under blotters? Are bulletin boards kept clear of classified matter?

5110. PUBLICATION SECURITY AND ACCOUNTABILITY

5111. CUSTODIAN

.1 A commanding officer shall designate, in writing, a Custodian of Registered Publications and a Publication Control Officer. These collateral duties will be assigned to commissioned officers.

.2 Custodial duties take precedence over all other collateral duties. Accordingly, an officer designated Custodian or Control Officer shall be limited in other duties so that he will have sufficient time to devote to the proper handling of publications in his custody.

.3 The duties and responsibilities of the Custodian of Registered Publications concern only registered publications and are listed in Chapter 3 of RPS 4. The duties and responsibilities of the Publication Control Officer concern those publications distributed through the Forms and Publications Supply Office (Code 4 publications) and are listed in OPNAV INSTRUCTION 5605.8 of 5 December 1957.

5112. ACCOUNTING AND DISTRIBUTION--REGISTERED PUBLICATIONS SYSTEM

.1 The Chief of Naval Operations has designated the Commanding Officer, U.S. Naval Security Station, 3801 Nebraska Avenue N.W., Washington 25, D.C., to operate a shipping, stowage, and accounting system known as the Registered Publications System (RPS) to meet the needs of the Navy in the distribution of registered pubs. All routine accounting reports and correspondence concerning accounting matters are to be addressed to the CO NAVSECSTA.

.2 An accurate and efficient system of transferring and accounting for cryptomaterial, which includes publications and devices, is essential to the maintenance of security. The custodian shall keep a systematic custody file and a current inventory of cryptomaterial whether in storage, in use, or on issue. It is the responsibility of each individual charged with the custody of cryptomaterial to know at all times the location of each document or device entrusted to his care and the purpose for which it is being used. The use of publications custody logs is advisable in order to maintain the strict accountability required when cryptomaterial is being turned over from watch to watch.

.3 In small Navy commands, the duties of custodian may be assigned the communication officer; in the Marine Corps, an officer from the adjutant section shall be designated. The custodian maintains the following standard files:

(a) Chronological file, which contains a copy of all transactions, accounting reports, and correspondence pertaining to registered publications. It is the central location within a command of all transfer reports (RPS-1), flyleaf receipts, destruction reports (RPS-2), inventory reports for transfer of custodian or change of command, and semi-annual inventories of registered publications for the periods ending 31 March and 30 September (RPS-16). The file may be subdivided into several file folders depending upon the amount of material involved.

(b) Custody card file, which is used to keep the status and custody record of individual registered publications. Everyone who draws a publication, including the commanding officer, signs for the publication on a custody card (RPS-17). When not in use, this file is kept in the vault.

5112.3 (Continued)

(c) Running inventory, which lists the short title of publications held, number of copies on board, and register numbers. The form also shows columns for remarks (changes, amendments or addenda) and disposition (method and date). The running inventory of publications held is a part of RPS-10.

.4 An officer should not assume custody or responsibility as custodian until he is certain that everything is in order. Similarly, an officer should not assume that he has been relieved as custodian until an itemized inventory and audit of everything he is responsible for has been taken and properly signed. The preparation and submission of such reports, including inventories, are detailed in Sections 6 through 9 of RPS 4. The following is a guide to some of the items that a relieving custodian should check:

Are publications charged to the command accounted for?

Is the chronological file properly maintained?

Are all copies of reports in the chronological file signed by all officers concerned?

Are all flyleaf receipts executed?

Is the custody card file properly maintained?

Is a status record maintained?

Have publications been destroyed at the right time?

Is the ship up to date on the drawing of publications from RPIO?

Is the authority to draw registered publications properly executed and up to date?

Are corrections to publications up to date?

Is knowledge of the main safe combination limited to two officers?

Does the commanding officer have a sealed copy of the main safe combination?

Does the destruction bill indicate priority of destruction?

Is the safe divided into ROB and EFFECTIVE sections?

Are sufficient weighted destruction bags provided where required?

Are weighted covers provided for cryptographic key lists?

.5 The distribution of registered publications is effected through the Registered Publications Issuing Offices (RPIOs) and Sub Issuing Offices established in or near naval district headquarters, naval shipyards, and other shore activities. Mobile Issuing Offices, located on board ships, issue publications to vessels in forward areas. Custodians shall maintain close contact with the nearest issuing office in order to keep up to date on publications and changes. A list of all RPIOs is contained in the Registered Publications Manual (RPM 1-1).

.6 Registered Publication Shipment Memoranda are sent by the Registered Publication Section to the issuing offices to provide information concerning distribution of publications. Ships and stations are not issued Registered Publication Shipment Memoranda.

5113. ACCOUNTING AND DISTRIBUTION--FORMS AND PUBLICATIONS SUPPLY OFFICE SYSTEM

.1 OPNAV INSTRUCTIONS 5605.6 and 5605.7 set up requirements for the inclusion of publications in the Registered Publications System, and set the distribution responsibility for publications not meeting these requirements with the Forms and Publications Supply Office (FPSO), operated by the Bureau of Supplies and Accounts.

.2 OPNAV INSTRUCTION 5605.8 contains complete instructions for the operation of a command's Technical Publication Library, the central control point within each command for the accounting, stowage, and use of Code 4 and other similar non-RPS-distributed publications. In the maintenance of this Technical Publication Library (TPL) it is the responsibility of the command to assure that all such publications are on board in accordance with the prescribed allowance, are corrected up to date, and are readily available for use.

.3 The position of Publication Control Officer is usually a collateral duty of the Classified Material Control Officer or the Administrative Officer. The Control Officer is responsible for the management and proper operation of the TPL. He is assisted by the Publication Clerk, a collateral duty assignment of an enlisted man or civilian whose primary duty station should be in the vicinity of the publication stocks and records. The Publication Clerk is responsible for the preparation and proper execution of all TPL transactions, record keeping, and such other duties as may be assigned in connection with the operation of the TPL.

.4 The functional components of the TPL are as follows:

(a) Publication Stock Center - The location of publications that have not been issued to TPL Holders. It is anticipated that most publications under control of the TPL will be drawn, maintained, and stowed by the cognizant offices. That office then becomes a TPL holder and is responsible for the maintenance and safe-keeping of the publication as long as it is retained.

(b) Custody Record File - A card file containing a TPL Catalog Card (OPNAV FORM 5070-11) for every basic publication under control of the TPL.

(c) Transaction File - A chronological file containing copies of all correspondence pertaining to the handling of publications in the TPL, including local memorandums, allowance lists, and Change Entry Certifications (OPNAV FORM 5070-12).

(d) Catalog of Publications - A locally prepared inventory of all publications in the TPL must be prepared annually just prior to the time of the annual administrative inspection, but may be prepared more often depending upon local circumstances. It should contain a list of all basic publications, showing the short titles, long titles, last changes or corrections entered, and number copies of all publications under control of the TPL.

(e) Publication Notices - A locally prepared memorandum used to advise interested offices of the receipt of new publications in the TPL. These notices plus a copy of the latest catalog (inventory) will inform all interested offices of the contents of the TPL.

5113. (Continued)

.5 Accounting for publications in the TPL is not required outside the command. But at least once a year a board shall be appointed by the command to inspect the operation of the TPL and the handling of all Code 4 publications within the command. The board shall consist of two persons, at least one member not connected with the TPL and senior to the Publications Control Officer. An inventory shall be prepared at this time and the board shall ascertain the following:

(a) that the inventory report is an accurate listing of the publications on board.

(b) that the authorized allowance of up-to-date publications is on board.

(c) that the records of the TPL are properly maintained.

(d) that adequate stowage is accorded classified matter, both in the TPL and by TPL holders.

.6 OPNAV INSTRUCTION 5605.7 contains complete instructions on the distribution, requisitioning, and stocking of those non-registered publications now the responsibility of FPSO. This instruction contains a list of Code 4 publications and a list of supply distribution points for areas previously served only by RPIOs. Publications authorized by an established allowance are ordered directly from the nearest FPSO supply point. If a holder feels that an increase in an established allowance is necessary, a letter request, including full justification, will be forwarded via the administrative chain of command to CNO (Op-28). If a publication is urgently required before a change in allowance can be obtained, a speedletter request will be submitted to CNO (Op-28) justifying the urgent requirement and stating that the publication is being drawn from the nearest FPSO supply point. Note that this is an emergency procedure only, and is not to be used to obtain an increase in allowance for every publication desired.

.7 Although the strict accounting procedures used in the RPS system are not required for Code 4 publications, the security requirements for this material are in no way minimized. All provisions of the Navy Security Manual (OPNAV INST 5510.1A) are applicable, in addition to the safeguards imposed by the proper administration of the Technical Publication Library.

5114. PUBLICATION ALLOWANCES

.1 A list of registered publications to be held by each class of ship or station, together with the number of copies authorized, may be obtained from the nearest RPIO. Allowance tables list all the registered publications of general distribution which are distributed by the Registered Publication Section through the issuing office.

.2 OPNAV INSTRUCTION 5601.1D contains similar allowance information and figures for all publications distributed by FPSO.

5115. ENTERING OF CHANGES AND CORRECTIONS

.1 Changes and corrections to publications are normally distributed through RPIOs or FPSO facilities. However, corrections by message, letter or memoranda may be otherwise promulgated.

5115. (Continued)

.2 Effective publications will be corrected immediately. Reserve-on-board registered publications will be corrected as soon as practicable as provided for in Article 314, RPS 4.

.3 Red ink should not be used for entering corrections since it becomes invisible when viewed under red battle lights.

5116. CORRECTION BOARD

.1 When the size of a command's allowance requires a large number of changes and corrections to be entered, a Correction Board may be designated by the commanding officer to assist the custodian.

.2 Members of the Board must follow the senior member's directions. The custodian normally is senior member.

.3 Even though a Board member enters corrections, it is the responsibility of the senior member to check the work for the entry of correct pages, etc.

5117. STOWAGE REQUIREMENTS

.1 Stowage requirements differ depending on the classification of the matter involved as set forth in Chapter 6, Section 1 of the SECURITY MANUAL.

.2 Until destroyed, superseded material is stowed in the same manner as required for effective material.

5118. HANDLING OF WORKING MATERIALS

.1 Work sheets, excess copies, typewriter ribbons, carbon paper and blotters used in preparing and processing classified information shall be accorded the same handling, storage and disposal as that exercised for other classified material. Separate sheets (not pads) of paper on hard surfaces shall be used when drafting or transcribing classified information.

5120. DESTRUCTION OF CLASSIFIED MATTER

5121. ROUTINE DESTRUCTION

.1 Publications shall not be destroyed prior to receipt of destruction authority from the Chief of Naval Operations, except in an emergency.

.2 The holder shall destroy superseded and obsolete publications when destruction orders are promulgated, unless a standard instruction or special correspondence authorizes retention.

.3 Routine destruction shall be completed promptly at the specified time in order that the amount of classified material subject to emergency destruction is kept at a minimum.

.4 The authorized methods of routine destruction and the reports of unauthorized destruction are discussed in Articles 227 and 317 through 320 of RPS 4.

5122. EMERGENCY DESTRUCTION BILL

.1 The commanding officer shall direct the preparation of an emergency destruction bill, the execution of which is an all hands evolution from communication officer to striker. Responsibility under the destruction bill shall be delegated by duty and watch rather than by

5122.1 (Continued)

name. Alternates for each billet shall be provided.

.2 Publications on board ships shall be stowed habitually in weighted perforated canvas bags. Material to be destroyed first should be marked in a distinctive manner.

.3 Emergency destruction of cryptomaterial shall be carried out in accordance with the emergency destruction bill. (Chapter 6, KAG-1.) Accurate records should be kept of all registered publications destroyed when at all possible to do so.

.4 Insofar as conditions permit, another officer should witness destruction. However, destruction should not be delayed to a point where it cannot be completed prior to sinking.

.5 The commanding officer shall ensure that adequate personnel are trained to act efficiently in an actual emergency. (See Chapter 6, SECURITY MANUAL.)

5123. REPORTS OF EMERGENCY DESTRUCTION

.1 Emergency destruction of cryptomaterial should be reported to higher authority immediately if communications exist. This is very important to future planning and operations. Plain language may be used as a last resort, quoting short titles only.

EXAMPLES:

(a) A plain language message from Shanghai on 7 Dec 1941 -

ALL COMMUNICATION PUBLICATIONS AND CONFIDENTIAL PAPERS DESTROYED EXCEPT DITOF.

(b) A plain language message from Guam on 9 Dec 1941 -

ALL CODES DESTROYED.

(c) An encrypted message from Corregidor on 6 May 1942 -

NOW DESTROYING ALL REGISTERED PUBLICATIONS AND MILITARY EQUIPMENT.

.2 When emergency destruction of classified communication material has been accomplished, a full report should be forwarded, as soon as possible, to the next senior in both the administrative and operational chains of command and also direct to the Chief of Naval Operations. The material destroyed, the method of destruction, and the extent of destruction of items not completely destroyed shall be indicated.

5124. UNAUTHORIZED DESTRUCTION

.1 Known destruction of publications without proper authority, either by accident or through a misinterpretation of authority, shall be reported in all cases without delay in accordance with Article 227 of RPS 4.

SECTION C

5200. CRYPTOSECURITY

5201. CRYPTOSECURITY OFFICER

.1 The commanding officer shall appoint an assistant communication officer for cryptosecurity who, through the communication officer, shall serve as advisor to the commanding officer in all matters relating to cryptosecurity and the physical security of cryptomaterials. He shall be responsible to the communication officer for the accurate, secure and efficient operation of the cryptocenter. In small commands the communication officer may serve as cryptosecurity officer.

5202. CRYPTOCENTER

.1 A cryptocenter is maintained, under direction of the cryptosecurity officer, for the purpose of having a secure place in which to encrypt and decrypt messages and store cryptomaterial (codes, ciphers and related publications) ready for immediate use.

5203. CRYPTOFILES

.1 Edited plain language copies of encrypted messages shall be stored as required for other material of the same classification except that copies of messages marked "PARAPHRASE REQUIRED" shall be stored in accordance with Article 0603 of the SECURITY MANUAL.

.2 Cryptocenter File. See Article 3001.2.

.3 Cryptoboard File. The cryptoboard may maintain a file of the encrypted version of all traffic sent to the cryptocenter. Each message contains a notation of the cryptoboard action. This file is divided into sections - incoming and outgoing. It may be kept on several boards in order to segregate scheduled files.

SECTION D

5300. TRANSMISSION SECURITY

5301. IMPROVEMENT OF TRANSMISSION SECURITY

.1 Transmission security is improved by the following:

(a) Circuit discipline and training.

(b) Defenses to minimize interception and direction finding.

(c) Defensive measures against traffic analysis.

.2 Detailed instructions relative to transmission security are contained in ACP 122.

5302. RELATIVE SECURITY OF TRANSMISSION

.1 Means and types of transmission in their order of security are generally as follows:

(a) Messenger.

(b) Registered mail-guard mail, U.S. Postal System or diplomatic pouch.

(c) Approved wire circuits.

(d) Ordinary mail-guard mail or U.S. Postal System.

(e) Nonapproved wire circuits.

(f) Visual means.

(g) Sound systems.

(h) Radio.

.2 Authorized personnel shall select the means most appropriate to accomplish the delivery of messages in accordance with the specified precedence and security requirements.

5303. TRANSMISSION OF TOP SECRET MESSAGES

.1 Top Secret messages never shall be transmitted by electrical means in the clear.

5310. DEFENSIVE MEASURES

5311. DEFENSE TO MINIMIZE INTERCEPTION AND DIRECTION FINDING

.1 Radio direction finders are effective on nearly all frequencies. A transmission of a very short duration is sometimes sufficient to permit a bearing to be obtained.

.2 Interception and direction finding can be made more difficult by:

(a) Avoiding unauthorized transmissions and unnecessary testing.

(b) Use of combinations of transmitters, antennas, and power which produce minimum wave propagation and emission intensity consistent with reliable communications.

5311.2 (Continued)

(c) Use of the broadcast method of transmitting traffic whenever possible in preference to the receipt method.

(d) Concealing instructions to shift frequency on tactical circuits by use of an encrypted message in the absence of a prearranged plan.

(e) Accurate transmitter adjustment and adherence to authorized frequency tolerances, thereby preventing the need for repetition of messages or parts of messages.

(f) Maintenance of strict circuit discipline.

5312. DEFENSIVE MEASURES AGAINST TRAFFIC ANALYSIS

.1 Traffic analysis is the technique of obtaining intelligence from the study of communications traffic without recourse to cryptoanalysis. It includes the statistical study of message headings, receipts, acknowledgments, relays, routing instructions and services; tabulation of the volume, types and directional flow at each point, and correlation of information taken from unclassified messages, noting departures from normality.

.2 A GUIDE to some of the measures which can be taken to render traffic analysis by the enemy more difficult and less reliable include:

(a) Minimum use of radio facilities when other means of communication are practicable.

(b) Maintenance of strict circuit discipline.

(c) Use of the broadcast method wherever possible.

(d) Rotation of frequencies.

(e) Rotation of unit call signs and address groups for encryption. Linkage between two types of call signs of the same unit, linkage of call signs with their plain language equivalents, or linkage of a unit and its associates through stereotyped addressals must be avoided.

(f) Minimum use of service messages, correction requests, and repetitions.

(g) Concealment of originating and addressed commands in the text of an encrypted message by use of Codress when authorized.

(h) Avoidance of long, easily associated messages of a recurrent nature by dividing into separate messages.

(i) Control of the timing and volume of test transmissions to avoid revealing information about impending operations.

(j) Keeping external routing instructions to a minimum.

(k) Avoiding use of plain language transmissions. Classified information transmitted via radio must be encrypted unless otherwise specifically authorized.

5313. DEFENSIVE MEASURES AGAINST IMITATIVE DECEPTION

.1 An enemy may attempt to enter communication nets employed by the Navy and simulate U.S. traffic in order to confuse and deceive U.S. and Allied forces. Such a practice is known as imitative deception.

.2 Imitative deception used against units frequently can be detected because in minor ways it lacks plausibility. The enemy's success or failure in imitative deception depends largely on unsuspecting communication personnel or on their haste and preoccupation in tactical situations.

.3 Communication personnel need to be alert for such enemy practices as the following:

(a) Combining the text of a genuine message, sometimes intentionally garbled, with the heading of another (word count corrected), and introducing it on a different radio net.

(b) Removing a message, sometimes including authenticators, from one circuit and introducing it on another circuit to waste time, create confusion, and produce service messages.

(c) Originating and transmitting false plain language messages.

(d) Calling a unit in the hope of taking bearings on the answering transmission. Communication personnel should be especially alert for this practice when radio silence is in effect.

(e) Arranging to have a false message partly obliterated by interference, usually to conceal lack of knowledge of authenticating or call signs.

.4 Defense against imitative deception is accomplished in the following ways:

(a) By thorough training in operating procedures as prescribed in Chapter Nine.

(b) By alertness of operators to recognize irregularity in procedures and characteristics of tone or keying.

(c) By direction finding on transmissions of questionable origin.

(d) By the minimum use of plain language and procedure messages.

(e) By the correct use of authentication.

5314. DEFENSIVE MEASURES AGAINST JAMMING

.1 An operator must be able to recognize jamming. He must deny the enemy any opportunity of determining the effectiveness of jamming.

.2 An operator must be aware of means to cope with a particular type of jamming. (Article 443, NWIP 16-1.)

5315. CIRCUIT DISCIPLINE

.1 Circuit discipline is that component of transmission security which includes the proper use of radio equipment, net control, monitoring and training; adherence to prescribed frequencies and operating procedure;

486999 O-58-7

5315.1 (Continued)

and remedial action. Lack of circuit discipline and lack of operator training in radio procedure, as well as negligence, inaccuracy and laxity, are responsible for the violations which endanger radio transmission security.

.2 Circuit discipline is attained by the following:

(a) Training in the use of proper operating procedures.

(b) Monitoring transmissions and instituting remedial action for security violations when and where necessary.

.3 Operating and maintenance personnel shall be trained to recognize and avoid the following malpractices which endanger communication security:

(a) Linkage or compromise of those call signs and address groups which are considered classified, by plain language or association with unclassified call signs.

(b) Linkage or compromise of encrypted call signs and address groups by association with other call signs, address groups or plain language. EXAMPLE: Use of encrypted call signs in the call, and unencrypted international or task organization call signs in the message address.

(c) Misuse and confusion of call signs, routing indicators, address indicating groups, and address groups. This may result in the non-delivery of an important message, a compromise or the linking of classified and unclassified call signs and address groups.

(d) Violation of CONELRAD conditions of silence and violation of visual silence.

(e) Unofficial conversation (chatter) between operators.

(f) Transmitting in a directed net without permission.

(g) Transmitting the operator's personal sign.

(h) Excessive repetition of prosigns or operating signals.

(i) Individual mannerisms in transmitting. The peculiar style of sending of an operator will frequently identify a unit or station even when frequency and call signs are changed. This applies to both transmitting and procedural peculiarities.

(j) Use of plain language in place of applicable prosigns or operating signals.

(k) Use of unauthorized prosigns.

(l) Unnecessary transmissions.

(m) Incorrect and unauthorized procedure.

(n) Identification of unit locations.

(o) Identification of individuals belonging to an organization.

(p) Excessively long calls.

(1) When a unit is called and does not answer within a reasonable time, presumably because a condition of radio silence prevails,

5315.2(p)(1) (Continued)

the message should be transmitted blind or put on an appropriate broadcast schedule.

(2) When a unit afloat calls a shore station on a ship-to-shore circuit and receives no answer within a reasonable time, the ship should deliver the message via any available station, using an indefinite shore station call sign if necessary.

(q) Failure to maintain radio watches on designated frequencies and at prescribed times.

(r) Transmitting at speeds beyond the capabilities of receiving operators.

(s) Use of excessive transmitting power.

(t) Tuning transmitters with antenna connected.

(u) Excessive time consumed in tuning, testing, changing frequency, or adjusting equipment.

(v) Use of excessive beam width or of a light larger or brighter than necessary.

.4 Use of profane, indecent or obscene language shall not be tolerated.

5316. OPERATOR TRAINING

.1 Encrypted messages transmitted by radio, wire and visual means for the sole purpose of training operating personnel may employ call sign ciphers and authenticators at the discretion of the officer conducting the exercise (OCE).

(a) Call sign ciphers will be employed in accordance with the effective call sign encryption plan.

(b) Texts of messages will consist of random undecipherable groups. System indicators will be taken from a list of DRILL indicators.

.2 Every plain language message transmitted by radio, wire or visual means solely for operator training will be identified by inclusion of the word DRILL at the beginning and end of the text.

.3 Encrypted or plain language messages for training exercises, command post or tactical exercises, or maneuvers, will be prepared in the same manner as normal traffic.

5317. MONITORING

.1 Stations and ships shall monitor their radio transmissions when practicable in order to reduce errors in procedure and violations of circuit discipline. Net control stations should monitor the transmissions of the net.

.2 Monitoring by central control agencies under area or higher commands provides a check on the effectiveness of monitoring by net control stations, but is not a substitute.

5320. PROTECTION OF MEANS OF TRANSMISSION

5321. RADIO PROPAGATION FACTORS

.1 Radio waves, regardless of the frequency or emission, are at times propagated over distances beyond the normal usable ranges.

.2 In particular, experience has shown that nominal line-of-sight distances at radio frequencies above approximately 30 megacycles are exceeded frequently. It may be assumed that, at times, signals may be propagated and intercepted:

(a) In the 30-100 band at distances exceeding 1000 miles;

(b) In the 100-500 band at distances of several hundred miles;

(c) Above 500 at distances of relatively less significance.

.3 It is essential that all concerned recognize the possibility of transmission of radio waves over extended distances, and maintain appropriate safeguards to prevent unauthorized interception.

5322. SECURITY OF RADIOTELEPHONE TRANSMISSIONS

.1 Careless or excessive use of radiotelephone is a serious hazard to communication security. Precautions in the use of radiotelephone are set forth in AFSAG 1248.

5323. SECURITY OF VISUAL TRANSMISSIONS

.1 Visual communication ordinarily is preferable to radio except when in close contact with enemy units at night.

.2 Transmission by visual means of a classified message in plain language shall be authorized only after careful consideration has been given to the necessity for sending in plain language and to the possibility of interception by unauthorized persons.

.3 Relative security of various visual systems:

(a) Day -

(1) Semaphore.

(2) Directional flashing light.

(3) Panels.

(4) Flaghoist.

(5) Pyrotechnics.

(6) Non-directional flashing light.

(b) Night -

(1) Infra-red communication systems.

(2) Directional flashing light.

(3) Pyrotechnics.

(4) Non-directional flashing light.

.4 The aperture of flashing light equipment shall be kept as small as

5323.4 (Continued)

practicable, particularly at night.

.5 In the interest of security, the following suggestions are offered:

(a) Train signal personnel to be the best lookouts on board.

(b) After establishing two-way communications, it is generally possible to dim the light for the remainder of the transmission.

(c) Use colored filters. They have been found effective for night use in areas when visual systems are permitted.

(d) Visual communication by flashing light should be avoided within five miles of land in order to eliminate the possibility of shining a light toward the shore.

(e) Use flaghoist in preference to flashing light for tactical signals. It is speedier and more secure.

(f) Classified messages to be transmitted visually should be encrypted if there is any possibility whatever of interception by enemy submarines, surface ships, aircraft or observers ashore.

5324. USE OF TELEPHONE

.1 Discussion of classified matter over any telephone system not equipped with security devices or approved for transmission of such matter is prohibited.

5330. AUTHENTICATION

5331. GENERAL PRINCIPLES OF AUTHENTICATION

.1 Authentication is a security measure designed to protect a communication system against fraudulent transmissions.

.2 Reliable systems of authentication are necessary to enable a receiving station to distinguish between genuine and fradulent stations or transmissions. Since imitative deception may be attempted at any time, it is necessary that stations be prepared to authenticate when required.

.3 A message cannot be rejected arbitrarily if its transmission was not authenticated, since authentication may not be required on all transmissions. Even incorrectly authenticated transmissions may be genuine. In situations where authentication is required, messages received incorrectly authenticated or unauthenticated are to be delivered locally without delay, but with suitable notations, for decision by the addressee as to their authenticity. When a message has to be relayed, the relaying station is to advise the receiving station that the message was not authenticated or was incorrectly authenticated.

.4 Only approved authentication systems are to be used.

5332. EMPLOYMENT OF AUTHENTICATION

.1 Authentication is mandatory under the following circumstances:

(a) When any station suspects imitative deception on a circuit.

(b) When any station is challenged or requested to authenticate. This shall not be interpreted as requiring stations to break radio silence for the sole purpose of accomplishing authentication.

5332.1 (Continued)

(c) When making contact and amplifying reports in plain language or brevity code.

(d) When transmitting a plain language cancellation of an encrypted category A message by radio, non-approved wire, or visual means (when sending stations cannot be recognized).

(e) When transmitting to a station which is under radio silence.

(f) When directing radio silence or requiring a station to break an imposed radio silence.

.2 Authentication is advisable under the following circumstances:

(a) When transmitting operating instructions which affect the military situation; for example, when closing down a station or watch, shifting frequency, or directing establishment of a special guard.

(b) When making initial radio contact. Authenticators should be exchanged to prevent an unauthorized station from opening a circuit by asking a legitimate station to authenticate.

5333. PROCEDURES FOR AUTHENTICATION

.1 Whenever an authentication system is promulgated, accompanying instructions shall specify the method of use and transmission procedure for use. Procedures will vary slightly with the form of authentication and the means of communication employed.

.2 Definitions of terms used in connection with authentication and methods for the use of authentication are prescribed in detail in AFSAG 1247.

SECTION E

5400. CENSORSHIP

5401. CENSORSHIP AUTHORITY

.1 Censorship of communications is a function of command.

.2 The authority to pass, delay, paraphrase, suppress, return for correction, or delete a portion of any communication is an essential form of protection of military information. This must be accomplished without undue delay in the speedy flow of communications so vital to the maintenance of good morale.

.3 Subject to the limitations contained in SECURITY, ARMED FORCES CENSORSHIP (OPNAV INST 5530.6), commanding officers have the absolute right to censorship over communications leaving their units. Where exercised, censorship may include personal communications, commercial traffic, press material, and messages for other Government agencies, as well as official messages of the Armed Forces.

.4 In all matters relating to censorship, ships and stations shall comply with the provisions of SECURITY, ARMED FORCES CENSORSHIP.

5402. PERSONAL CENSORSHIP

.1 Automatic censorship of official and unofficial conversation and letters is a fundamental duty of all personnel of the Naval Establishment. The habit must be cultivated until it becomes routine.

5403. UNIT CENSORSHIP

.1 The commanding officer of each unit may appoint one or all of the officers in his command to be unit censors.

.2 Unit censors have cognizance over all outgoing communications, with the exceptions noted in paragraphs 21 and 26 of SECURITY, ARMED FORCES CENSORSHIP.

.3 All personal communications are subject to wartime armed forces censorship.

.4 Information which is prohibited from appearing in personal mail is listed in paragraph 20(d), SECURITY, ARMED FORCES CENSORSHIP.

5404. PRESS CENSORSHIP

.1 In circumstances where security control of information is necessary but formal press censorship has not been established, press representatives will be requested to cooperate voluntarily to prevent revelation of intelligence to the enemy. In such circumstances, commanding officers and their representatives must be unusually alert to the doctrine of security at the source to prevent inadvertent disclosure of information.

(a) At any time when doubt exists as to the desirability of releasing press material, such material should be forwarded through appropriate classified channels to the fleet commander or higher authority for decision.

.2 When formal press censorship, either voluntary or involuntary, is invoked by appropriate authority, full responsibility for censorship of press material is exercised through Navy field press censors.

5404.2 (Continued)

(a) Generally, the only press material that need be censored at the scene of action is that which may be transmitted by radio. This press material will be censored by the Navy field press censor assigned to the transmission point or any other Navy field press censor at the scene of action. Other material may be forwarded uncensored to transmission points outside the immediate combat area for censorship and transmission.

(b) Neither fleet public information officers nor officers with collateral duty as public information officers will perform press censorship. Unit censors are specifically prohibited from censoring press material unless specifically authorized by proper authority.

(c) In order to expedite delivery from point of origin to censorship and transmission points at the scene of action, when radio transmissions are permitted, press material may be transmitted in an uncensored status by very high frequency, ultra high frequency, super high frequency, or extremely high frequency when it is apparent that no assistance to the enemy will accrue thereby.

.3 Disclosure of information through public relations is discussed in Chapter 10 of the SECURITY MANUAL.