AFSAG 1248

File

NONREGISTERED

~~CONFIDENTIAL~~

Security Information

FUNDAMENTALS OF TRANSMISSION SECURITY-JOINT

This document consists of cover and 60 numbered pages
1 to 66 inclusive

Verify presence of each page upon receipt

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D. C.

SEPTEMBER 1952

~~CONFIDENTIAL~~

ORIGINAL
(Reverse Blank)

AFSAG 1248

NONREGISTERED

~~CONFIDENTIAL~~

Security Information

FUNDAMENTALS OF TRANSMISSION SECURITY-JOINT

This document consists of cover and 66 numbered pages
1 to 66 inclusive

Verify presence of each page upon receipt

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D C

SEPTEMBER 1952

~~CONFIDENTIAL~~

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D C

1 September 1952

FUNDAMENTALS OF TRANSMISSION SECURITY - JOINT

LETTER OF PROMULGATION

1 AFSAG 1248 is a CONFIDENTIAL, Nonregistered Publication and will be handled, stored and accounted for in accordance with current regulations of each Service

2 AFSAG 1248 will become effective upon receipt Instructions for the eventual disposal of AFSAG 1248 will be issued at an appropriate time by the Director, Armed Forces Security Agency, through normal Service channels

3 Changes to this publication will be promulgated by means of a letter, memorandum or message and are to be entered upon receipt The individual entering the change shall so indicate on the Record of Corrections page included herein as page 3

4 This publication is issued to those units designated by the Director, Armed Forces Security Agency, the Chief, Army Security Agency, the Director, Naval Communications, and the Commanding General, U S Air Force Security Service

5 THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U S C , SECTIONS 793, 794 AND TITLE 50, U S C , SECTIONS 46, 46a AND 46b ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW

6 EXTRACTS FROM THIS DOCUMENT MAY BE MADE IF NECESSARY SUCH EXTRACTS WILL BE SAFEGUARDED IN ACCORDANCE WITH CURRENT SERVICE REGULATIONS

7 This publication will not be carried in aircraft for use therein

RALPH J CANINE
Major General, US Army
Director, Armed Forces Security Agency

RECORD OF CORRECTIONS

Identification of Correction or Change and Reg No (if any)	Date Entered	By whom entered (Signature, rank or rate Name of Command)

TABLE OF CONTENTS

CHAPTER 1

GENERAL

CHAPTER 2

TRANSMISSION SECURITY IN COMMUNICATION PLANNING

CHAPTER 1

GENERAL

1000 - INTRODUCTION

1001 PURPOSE — Fundamentals of Transmission Security - Joint, AFSAG 1248, has been prepared to formalize and promulgate those principles of transmission security necessary for communication planning and operation

1002 APPLICATION

a The effectiveness of transmission security measures is dependent upon coordinated and consistent application of security principles in all phases of communications Those responsible for transmission security (commanders) and those through whom the responsibility for transmission security is fulfilled (communication and signal officers) must be cognizant of any aspect of communications which affects transmission security, whether it is communication planning, message drafting, communication operations, or security monitoring AFSAG 1248 provides the basis for such coordinated and consistent application of transmission security principles

b AFSAG 1248 provides a standard reference for those engaged in preparation and implementation of communication plans and operating procedures Principles set forth herein are incorporated in Communication Instructions (JANAP/ACP) as appropriate, but the contents of this manual are not to be construed to prohibit changes in Communication Instructions to those procedures which are of a purely operational nature AFSAG 1248 also provides a guide for use in training personnel in the provision and maintenance of transmission security

1003 COMMENTS — Comments regarding any portion of AFSAG 1248 are invited and should be submitted to the Director, Armed Forces Security Agency, Washington 25, D C , through Service channels

11ØØ - DEFINITIONS AND RESPONSIBILITIES

11Ø1 TRANSMISSION SECURITY — Transmission security is that component of communication security which results from all measures designed to protect transmissions from unauthorized interception, traffic analysis, and imitative deception

a Interception — Interception is the process of obtaining communications intended for others All communications are subject to interception in transmission, but some means of transmission are inherently more secure against interception than others Interception has as its ultimate purpose the derivation of intelligence

b Traffic Analysis — Traffic analysis is the study of the external characteristics of communications and related materials, without recourse to cryptanalysis, for the purpose of obtaining information concerning the organization and operation of a communication system This information is used (1) as a basis for drawing deductions and inferences of value as intelligence, even in the absence of specific knowledge of the contents of the transmission, (2) as an aid to cryptanalysis, (3) as a guide to efficient intercept operations, and (4) as a basis for imitative deception

c Imitative Deception — Imitative deception is the introduction of fraudulent transmissions, in imitation of authentic transmissions, into communication channels of an opposing force Such fraudulent transmissions may be designed to create confusion, to influence tactical operations, or to penetrate communication security

11Ø2 JOINT APPLICATION OF TRANSMISSION SECURITY MEASURES — The increasing use of joint communication facilities and frequent unpredictable transfer of communications from the facilities of one Service to those of another Service make standardized application of transmission security measures, and use of standardized communication operating procedures, essential to effective and secure communication Joint communication policy, joint communication instructions, and joint security methods and operating procedures should be used by all Services for all communications, whether joint or intra-Service

11Ø3 RESPONSIBILITY FOR TRANSMISSION SECURITY

a Individuals — Every individual engaged in the transmission of communications, or the preparation of communications for transmission, is responsible for compliance with authorized procedures governing preparation, transmission, and safeguarding of communications

b Command — The implementation of transmission security policies and procedures is a command responsibility extending from the high command of each Service to every commander having cognizance of communication transmissions Commanders are responsible for the execution of communication security measures prescribed by higher authority as applicable to the means of communication employed Command responsibilities include the training, monitoring, and remedial action which are required for the successful implementation of transmission security policies and operating procedures

(1) The responsibility for the maintenance and improvement of transmission security is fulfilled at all echelons of command through communication or signal officers who formulate local regulations in conformance with policies and procedures directed by higher authority, and who supervise communication operations to assure the maintenance of transmission security All echelons of command shall review communication directives issued by their subordinate echelons to insure uniformity and standardization of communication methods and procedures within their respective commands

(2) Net control stations are designated by appropriate authority to direct and control the operation and flow of all traffic handled on a communication net The station serving the senior command is normally designated as the Net Control Station It may be any station in a net, however, which can best fulfill the functions of maintaining net discipline and clearing traffic expeditiously Net control stations should monitor transmissions in the net to assure the fulfillment of operational and transmission security requirements

c Service Cryptologic Agencies and Communication Security Activities — Intra-Service evaluation of the adequacy of transmission security measures and effectiveness of their application is the responsibility of Service cryptologic agencies and their Communication Security Activities These agencies include the Army Security Agency, the Naval Security Group, and the Air Force Security Service These organizations have the capability to monitor and analyze friendly transmissions for the purpose of determining what intelligence is available to the enemy and what countermeasures are required In the process of evaluation, considerable information becomes available which is of great assistance to commanders in implementing prescribed security policies and communication operating procedures For this purpose, security violations and discrepancies in application of communication operating procedures are reported to the responsible command

d Director, Armed Forces Security Agency — The Director, Armed Forces Security Agency, is charged with the responsibility for formulation of transmission security policies and doctrine He also serves as a coordinating authority for Service cryptologic organizations and exercises technical supervision over their Communication Security Activities

e Joint Communications-Electronics Committee — The responsibility of the Joint Communications-Electronics Committee for transmission security is embodied in those functions of the Committee which are concerned with the establishment of principles, policies, and plans for joint communications-electronics and the establishment of communications-electronics methods and procedures

12ØØ - MILITARY NECESSITY FOR TRANSMISSION SECURITY

12Ø1 GENERAL — The communications necessary to effect control and coordination of the complex elements of military operations are a source of much vital military information to any opposing force which can intercept and analyze them Classified military communications require physical protection at all times to deny unauthorized persons access to the communications When prevention of interception cannot be assured in the transmission of classified communications, they must be encrypted to make them unintelligible to unauthorized persons Since the organization of the communication system necessarily represents the disposition of military forces, and since much military intelligence is available by implication from the external characteristics of traffic and the circumstances of transmissions, special effort must be made to minimize unauthorized interception and to reduce the amount of intelligence available through analysis of electrical transmissions

a Value of Communication Intelligence — The derivation of military intelligence through analysis of insecure communications is economical of time and manpower and is often more reliable than other means of collecting intelligence Radio intelligence organizations exploit this source of intelligence, and military communications are, therefore, subject to intensive analysis

b Vulnerability of Peacetime Communications — The basic data necessary for successful communication intelligence operations can be compiled in peacetime when security precautions are relaxed and the civil and military communications structure and procedures can be observed freely Commercial and amateur radio communications and the nets of the merchant marine, the non-military facilities, and other internal communications are studied for the military significance of conversion to wartime uses

c Protection of Military Communications — Military operations require effective transmission security to prevent or limit the derivation of military intelligence from communications through unauthorized interception and traffic analysis Although communications can be intercepted and analyzed by many varying and ingenious methods, that which is highly successful in one case may be worthless in another The protection of communications depends upon a thorough understanding of the possibilities for deriving communication intelligence and an appreciation of the most hazardous aspects of any given communication situation in order that the protection most needed in that particular situation may be recognized and provided

12Ø2 INTELLIGENCE AVAILABLE THROUGH TRAFFIC ANALYSIS — A military force seeks any intelligence which will enable it to achieve military advantage over an adversary Military advantage may be achieved by a favorable disposition of forces against the known opposing order of battle, or by leading the opponent to make unfavorable disposition of his forces Intelligence which makes such military advantage possible is latent in the external characteristics of the military communications of an opposing force and can be obtained by traffic analysis to a greater or less extent, depending upon the skill of analysts, volume of traffic available for study, the effectiveness of security precautions and the collateral information available to analysts

a Order of Battle — In the absence of adequate transmission security measures, a communication organization, which is a medium of command, reflects the underlying military organization, and the flow of traffic within established communication channels manifests the military plans and operations which make communications necessary The operational structure, grouping, and intentions of the military force in a specific area of operations often can be determined through traffic analysis and reconstruction of the communication organization

b Military Plans and Operations

(1) Unit movements and preparations for military activity may be indicated by rising and falling traffic volumes and changes in the structure of the network

(2) The military function of a network may be revealed by the characteristic traffic pattern which results from transmissions incidental to planning, supply, or transportation Such patterns can be exposed through tabulation and analysis of transmission components and correlation with related intelligence from sources other than communications

(3) Change of grouping, disposition of forces and fleets, and probable tactical developments may be manifested in the redeployment of the radio stations which serve military elements

c Information Regarding Research and Development of New Weapons or Techniques of Warfare — Intelligence of research and development conducted by an opposing force can be produced from communication transmissions by the collection of fragments of information which may be insignificant individually but which provide intelligence when combined and considered in relation to information from other sources

d Detailed Knowledge of Opponents's Communication System — Detailed knowledge of the operation and organization of an opponent's communication system serves as the means of achieving military advantage by providing the basis for effective intercept and imitative deception

(1) Significant military information can be obtained from communications only when intercept facilities and personnel can be employed on the circuits most productive of the type of traffic desired The detailed knowledge of the operation and organization of a communication system, which can be derived through traffic analysis, provides a guide to intercept When the external characteristics of traffic indicate the transmission of information of particular interest, or when a certain type of encryption can be solved, intercept can be directed to the circuits where such transmissions can be obtained and a greater volume of informative traffic is made available for study A detailed knowledge of the circuits (frequencies used, etc) makes effective intercept possible

(2) Familiarity with the organization and operation of the communication system also makes it possible for an enemy to imitate authentic transmissions convincingly This ability gives him the opportunity to confuse and delay communications, mislead commanders in tactical evaluation, and induce stations to break radio silence or violate other security regulations

e Cryptographic Information — Portions of the text of encrypted messages often can be assumed from external features when a stereotyped message can be recognized or the probable originator and addressee are determined through traffic analysis Such information may greatly facilitate the work of cryptanalysts and assists in penetrating the protective disguises of the victim communications

13ØØ - MEANS OF PROVIDING TRANSMISSION SECURITY

13Ø1 GENERAL — Circuit discipline, that is, operation in accordance with prescribed procedures and habitual observation of security regulations, has an important bearing on the security of electrical transmissions (radio, wire, and some visual means) Operating procedures and security regulations have been formulated through experience and research to accomplish accurate, secure, and efficient delivery of messages To assure the protection which they afford, circuit discipline must be maintained constantly Circuit discipline is maintained by training, monitoring, and necessary remedial action

13Ø2 TRAINING — All personnel concerned with communications must be thoroughly trained to appreciate the necessity for security measures Normally, operators receive detailed instruction in communication operating procedures and security requirements in Service schools before assignment as communication operating personnel This training must be supplemented and maintained constantly by the organization of assignment Replacements in the field must be trained locally Commanding officers of Naval elements may request communication security activities to pay "training visits" to fleet units and activities for which the commander is responsible The Army and the Air Force have organizations performing similar functions Such visits provide constant training and opportunity for discussion of questions regarding procedure and any irregularities found in the communications of a particular station Security indoctrination of message originators must be accomplished through command channels

a Encrypted Traffic for Training Purposes

(1) Encrypted messages for training are for four general purposes

(a) Classroom training

(b) Radio, visual, or wire operator training

(c) Cryptopersonnel training

(d) Maneuvers

(2) These four types shall be treated as follows

(a) For classroom training, cryptosystems designated as "Training Systems" will be used Since "Training Systems" are seldom, if ever, superseded, messages prepared using these systems shall not be transmitted by radio, wire, or visual means

(b) Messages transmitted by radio, wire, or 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 drill, in this event only effective editions will be used Call sign ciphers will be employed in accordance with the effective call sign encryption plan Texts of messages will consist of random undecipherable groups, and system indicators will be taken from a list of "drill" indicators which have the meaning "The following text consists of random undecipherable groups"

(c) Messages which are encrypted for the purpose of training cryptopersonnel and which are transmitted by radio, visual, or wire means will employ effective call sign ciphers and authenticators if such are prescribed for normal communication The system indicators used will be those assigned for drill purposes only to the various cryptosystems, and having the meaning, "The following text is for cryptodrill purposes only" The text of the messages will be encrypted in the effective edition of the appropriate cryptosystem, except where a special practice edition is available As added safeguards, in addition to the special indicator, the following precautions will be effected

1 Text must have no relation to current operations, must be of free composition, and must not consist of verbatim quotation from a newspaper or other printed document

2 All operating procedures required for the normal use of the system must be fully observed

3 Messages will be so worded that texts cannot be interpreted as other than cryptopersonnel drill messages

4 Measures will be taken to insure that cryptopersonnel drill messages do not fall into routine distribution channels

5 All plain language copies of cryptopersonnel drill messages will be marked across the face "cryptopersonnel drill message"

(d) Encrypted messages for training exercises, command post or tactical exercises or maneuvers

1 This traffic will be prepared in the same manner as normal traffic

2 When such traffic makes reference to a simulated enemy, such as in contact or amplifying reports, a procedure for identifying such traffic shall be used in order not to alarm units not engaged in the exercise or maneuvers, the officer conducting the exercise or maneuver shall include appropriate instructions in the order or plan for the conduct of the exercise or maneuver Normally this procedure will consist of the use of some fictitious designation assigned to the opposing forces such as Black Force, White Fleet, etc Example "Black Force previously reported is now withdrawing" If some procedure equivalent to that illustrated above is not used, the originator will include the word "Exercise" at the beginning and end of the text

b Plain Language Traffic for Training Purposes

(1) Plain language transmissions for training purposes are of two types

(a) Traffic transmitted solely for operator training

(b) Traffic transmitted during the conduct of maneuvers or exercises

(2) These two types shall be treated as follows

(a) Every plain language message transmitted by radio, visual, or wire means solely for operator training will be identified by inclusion of the word "Drill" at the beginning and end of the text

(b) Plain language transmissions by radio, visual, or wire means during the conduct of training exercises, command post or tactical exercises, or maneuvers, will be prepared in the same manner as normal traffic When, however, such traffic makes reference to a simulated enemy such as in contact or amplifying reports, a procedure for identifying such traffic shall be used in order not to alarm units not engaged in the exercise or maneuvers, the officer conducting the exercise of maneuvers shall include appropriate instructions in the order or plan for the conduct of the exercise or maneuvers Normally this procedure will consist of the use of some fictitious designation assigned to the opposing forces such as Black Force, White Fleet, etc Example "Black Force previously reported is now withdrawing" If some procedure equivalent to that illustrated above is not used, the originator will include the word "Exercise" at the beginning and end of the text When using radio transmitters of limited range, employing voice transmission, responsible officers may dispense with the precaution outlined above

1303 MONITORING — Monitoring (surveillance of one's own communications) serves two major purposes

a Basis for Countermeasures — Monitoring and subsequent security analysis provide information which is of value to the commander by indicating what communication intelligence is available to the enemy and what countermeasures are required

b. Basis for Improvement of Communications. — Monitoring and subsequent security analysis serve to apprise the responsible commander of discrepancies in application of communication operating procedures and violations of transmission security, and indicate what training and corrective measures are needed to assure compliance with prescribed communication operating policies and procedures.

13Ø4. REMEDIAL ACTION.

a. Improvement of Circuit Discipline. — Remedial action taken as a result of security monitoring may be directed towards improvement of circuit discipline and transmission security by:

(1) Intensive training of operators to correct discrepancies in operating procedures or violations of security revealed by monitoring.

(2) Directives and instructions to message originators and drafters to eliminate insecure practices.

b. Revision of Communication Operating Policies and Procedures. — Remedial action also may be directed towards revision and improvement of communication operating policies and procedures prescribed for use. This is accomplished through security representation of appropriate panels of the Joint Communications-Electronics Committee.

CHAPTER 2

TRANSMISSION SECURITY IN COMMUNICATION PLANNING

2000 - INTRODUCTION

2001 GENERAL COMMUNICATION PLANNING — Transmission security requirements are incorporated in broad communication planning at higher echelons, and Service regulations prescribe means of transmission to be used for specific communication situations peculiar to the Service, but the formulation of the details of communication planning is the duty of unit signal or communication officers, who must interpret the overall plan in terms of local requirements and capabilities

2002 LOCAL COMMUNICATION PLANNING — Local communication operating instructions prepared by communication officers and signal officers must provide for transmission security as necessary to meet the communication requirements of a commander's plans Reliability, security, and speed are requisite elements of all military communications The relative importance of security and speed, and the relative security of different means of transmission, vary with the circumstances Unit signal or communication officers, therefore, must be guided by operational requirements and limitations and a consideration of security principles applicable to the means of transmission available in the particular situation

21ØØ - GENERAL REQUIREMENTS

21Ø1 CALL SIGNS, ROUTING INDICATORS, AND ADDRESS DESIGNATIONS — One of the primary objectives of traffic analysis is reconstruction of the operational organization of the opposing force Solution of call sign systems, with identification of call signs and address designations, is the principal means of determining operational organization and, accordingly, is an essential task of the enemy traffic analyst Measures to hinder or delay solution of call sign systems and identification of call signs thus become of utmost importance in the achievement of transmission security

a Determination of Security Requirements — The necessity for protective measures is based entirely on consideration of the value of the available information to the enemy, and the effects of compromise of the information on the overall military effort Since individual originators frequently do not have knowledge of other than the local situation, they are not in a position to evaluate comprehensively the effects of compromise on the overall military effort and consequently are unable to determine uniformly their own security requirements or the requirements of those with whom they may communicate Therefore, the necessity for protection and the degree of security required ordinarily must be determined on an area-wide or world-wide basis The uniform application of security measures also has become essential as a result of the increasing integration of communication facilities to meet the global requirements of military communications Unless every command conforms with the maximum requirement of other commands with whom communications are conducted, compromising linkages are inevitable This need for comprehensive evaluation of the security requirement and uniform application of security measures makes it advisable that most security measures be prescribed on a world-wide basis Accordingly, the responsibility for determining the security means to be employed and the extent of application is vested in the Chiefs of the Military Services Fulfillment of this responsibility is accomplished intra-Service through the chief of the appropriate cryptologic agency and jointly through the Director, Armed Forces Security Agency In those cases where application on a limited basis or in a limited area (e g , theater) is feasible, the authority to implement a designated security means may be specifically delegated to the commander having cognizance over all commands concerned

b Protective Methods — Several procedures or means can be employed to provide varying degrees of protection for call signs and address designations The effectiveness of each is dependent to a considerable extent upon adherence to rules and procedures governing their use Selection of the means or procedure to be employed is based upon such factors as the length of time for which protection is required, conjunctive operating procedures and communication facilities, type of call sign involved, the probabilities of compromise through non-communication sources, the operating conditions involved, the physical protection possible for the particular means to be employed, etc

(1) Physical protection for call sign and address designation assignments is provided by classification and registration Basic call signs for use by the Armed Forces are contained in the JANAP/ACP Call Sign Series Extracts and re-allocations of call signs from these publications should be classified and handled in accordance with classification and handling requirements for the basic document Classification alone, however, normally does not afford adequate protection It is the initial step toward provision of protection

(2) Call sign encryption, employing a call sign cipher device and daily changing keys, has proved to be the most effective and practical means yet devised for obtaining call sign security in situations where promulgation of frequent changes to basic allocations is impracticable and where an appreciable amount of physical protection can be afforded the keying material Security provided by call sign encryption is enhanced by application of additional measures such as maximum use of broadcast type transmissions, use of indefinite call signs as originators, use of variants as bases for encryption, etc

(3) Daily or frequent rotation of call signs in a completely random manner is used to provide protection under conditions which make any form of encryption impracticable and where requirements for knowledge of assignments can be localized to a specific area or element of command This means is particularly useful for ground forces engaged in combat operations, ground elements of air forces, and, in some cases, air units engaged in tactical operations Since the communications of such forces are likely to be limited to a particular theater or area of operations, application may be made on a correspondingly limited basis without affecting operations in other

theaters or areas Whenever possible, call sign changes should coincide with changes of frequency, serial number series, and other identifying characteristics to prevent linkage between old and new call signs

(4) Codress provides for the indication of specific addressees and originators within the encrypted text rather than in any external identification Codress provides the maximum possible security for communications when the radio calls employed in transmission do not serve to identify the originator and the addressee, and when other identifying characteristics are not present It is an extremely useful method to avoid revealing associations on multiple-address messages Codress may be employed at any time unless specific Service instructions have been issued to prohibit its use

(5) On certain teletypewriter circuits, on-line cryptosystems may be used to encrypt the entire headings of messages as well as the text, thus providing completely effective protection for address designations and routing indicators Operational considerations, i e , equipment, personnel, circuit conditions, etc , impose considerable limitations on use of this highly effective protection at present, but its use should be extended wherever feasible

(6) Use of F, or broadcast, type of transmission is an effective means of enhancing security when used in conjunction with other means designed to protect the identities of specific addi essees, particularly when radio calls are synonymous with addressee designations

(7) Indefinite call signs are an extremely effective means of achieving protection for the identity of specific originators in circumstances where operating conditions permit their use They are employed normally as a supplemental means of protection when a requirement exists for the encryption of address designations

(8) Use of collective call signs or address indicating groups may provide an effective means of protection against continuity afforded by stereotyped multiple-address patterns, in that no specific indication of the number and identity of addressees is provided on any single transmission The security achieved through use of this means can be greatly enhanced by the application of additional protective measures such as encryption

(9) Variant call signs to represent the same command or communications facility ordinarily provide, at best, extremely limited protection, since variants may be equated quickly by traffic analysts Variants are assigned and must be used, however, for those call signs which are subject to encryption This is necessary to increase the security provided by the call sign cipher device

(1Ø) In situations where an extraordinary degree of protection is required, special cover procedures can be devised for the purpose of deceiving enemy analysts This may be accomplished by arranging for filing and delivery by apparent originators and addressees which in reality are quite different from the actual addressees or originators Such procedures usually will be planned and implemented only by specially trained communication security personnel

21Ø2 SERIAL NUMBERS — In planning the use of any system of external sei ial numbers for convenience in the handling of traffic by code rooms, signal centers, originating units, radio stations, etc , the security hazards of serial numbers should be considered The traffic continuity which is indicated by serial numbers may link changing call signs, transmission schedules, or frequencies, and thus provide the means of determining traffic volumes and maintaining continuity of intercept In comprehensive communication planning, the increased facility of operation which serial numbers provide must be weighed against the undesirability of disclosing such information to the enemy

21Ø3 CRYPTOGRAPHIC SYSTEMS — Cryptographic systems may be characteristic of echelon, and the structure of enciphered transmissions may indicate subordination of a radio station to a particular country or Service, if individual systems of encryption are used by the different elements

of combined and joint operations Elimination of such distinguishing differences may not be practicable, but the information revealed by such usage should be recognized

2104 AUTHENTICATION SYSTEMS — When an authentication system has not been prescribed for general use by competent authority, authentication systems are formulated locally in accordance with AFSAG 1247 Local instructions must describe the method of use of authentication systems, specify the test elements to be used, and, if a time element is used, whether GMT or local zone time is to be used

2105 RESERVE OPERATING INSTRUCTIONS — Provision for undistributed reserve communication operating instructions incorporating alternate authentication systems, call sign and frequency assignments, and other security measures, is an important contribution to transmission security in the event of physical compromise of the entire effective communication operations instructions through loss or capture

2106 TEST TRANSMISSIONS — Timing and volume of test transmissions during rehearsals for military operations must be controlled to avoid revealing information about impending operations

2107 COMMUNICATION SILENCE — Under certain conditions (such as impending military movement or operations), commanding officers may sacrifice the convenience and speed of electrical communication (particularly radio and visual means) in the interest of maximum security to conceal such information as the presence, number, and movement of troops, ships, or aircraft Controlled communication silence should be imposed in conjunction with radar, IFF, and electronic countermeasure silence as well as other protective measures which decrease the intelligence available to the enemy Prior to resuming normal operations, strict control of test transmissions must be effected

2108 TRANSMISSION OF CLASSIFIED INFORMATION

a Approved Circuits — An approved circuit is a circuit of a particular electrical means of communication which has been approved by proper authority for the transmission of classified information of a specified security classification The term "classification rating" denotes the highest security classification of plain language messages for which the circuit is approved (not to be confused with the security classification of the existence of such a circuit) Approved circuits will not afford security equivalent to that obtained by the use of an appropriate cryptosystem and shall not be considered as a permanent substitute for cryptographic provisions Maximum use of existing cryptographic facilities will be made in preference to using approved circuits Specific policies regarding approval of radio, wire, and visual circuits are contained in paragraphs 2206, 2302, and 2403, respectively

b Nonapproved Circuits — A nonapproved circuit is any electrical circuit not specifically designated as an approved circuit by competent authority Classified traffic transmitted over nonapproved circuits will always be encrypted with the following exceptions SECRET, CONFIDENTIAL, or RESTRICTED information may be transmitted in plain language over nonapproved circuits only in the following cases

(1) Over any nonapproved circuit in tactical operations (actual or simulated) when speed of delivery is so essential that time cannot be spared for encryption and the transmitted information cannot be acted upon by the enemy in time to influence current operations In such cases, each transmission in plain language must be individually authorized by the commanding officer or his specifically authorized representative

(2) Over a visual circuit after careful consideration has been given to the necessity for sending in plain language and to the possibility of interception by unauthorized persons In such cases, each transmission in plain language must be individually authorized by the commanding officer or his specifically authorized representative

c TOP SECRET security information shall never be transmitted in plain language over any electrical circuit under any conditions

22ØØ - RADIO TRANSMISSION SECURITY

22Ø1 NATURE OF RADIO TRANSMISSIONS — Radio transmissions include radiotelephone, radiotelegraph, radioteletypewriter, radiofacsimile, and radio television The speed and traffic volume capacity of radio makes it highly desirable for communications at both strategic and tactical levels The major disadvantage is that radio usually is the least secure of all means of transmission The unauthorized reception and recording of radio transmissions cannot be detected or conclusively prevented Radio transmission security therefore, depends upon transmission in such a manner that maximum effort is required for the accomplishment of unauthorized interception and analysis

22Ø2 INTERFERENCE WITH RADIO TRANSMISSIONS — Radio communication is vulnerable to interfering electronic transmission, both unintentional and intentional

a Unintentional Interference — Unintentional interference results from such things as atmospherics and equipment failures Such effects can usually be reduced or avoided by careful planning

b Intentional Interference — Intentional interference (jamming) is the intentional radiation of electronic transmissions with the object of reducing the effectiveness of specific electronic equipment Its use is reciprocal and it may be used as an aid to interception and analysis by forcing the repetition of messages and lowering circuit discipline

22Ø3 RANGE OF RADIO TRANSMISSIONS — Consideration of factors influencing the range of transmissions is essential in any attempt to limit the interception or jamming of radio transmissions Among these factors are such things as the nature of the transmission path, atmospheric conditions, frequencies used, and the equipment employed The limitations of frequency, terrain, and equipment often can be approximated, and every effort should be made to provide the minimum wave propagation and emission intensity consistent with reliable communication In so doing, however, it must be realized that atmospheric conditions, which affect the range of transmissions and often result in the extension of radio waves far beyond their normal limits, cannot be detected or anticipated at all times Line-of-sight distances characteristic of VHF and higher frequency transmissions are frequently exceeded as a result of abnormal and unpredictable ionospheric and meteorological conditions

22Ø4 ASSIGNMENT OF FREQUENCIES

a Defense Against Traffic Analysis

(1) Provision for variation of frequency in a network permits much more secure communication operation than is possible when stations are compelled to operate on unchanging or severely limited frequencies When frequencies are not changed they may serve to identify stations even though operations are disguised by the use of changing call signs, changing time of transmission, etc The changed elements often can be correlated to unchanged frequencies to assure continuity of interception

(2) Any pattern in the assignment of frequencies should be avoided to prevent the possibility of identifying the source of traffic on the basis of frequency alone

(3) Rotation of frequencies used within a network is the most effective means of preventing station identification through frequency The number of frequencies available for use is often very limited, and the rotation of frequencies complicates communication operations If these disadvantages can be overcome, however, and frequency can be changed when call signs and times of transmission are changed, the system of assignments and use of frequencies can be determined only by the analysis of much greater volumes of traffic and the interception and analysis of traffic is greatly delayed and complicated

b Defense Against Intentional Interference — Employment of widely separated frequencies enables communication networks to evade jamming and to prevent concentrated jamming efforts in a limited range from interfering with all communication in the net If jamming efforts can be forced to cover a wide range of frequencies, the resulting loss of efficiency greatly lessens the effectiveness of jamming Provision for rapid changes in operating frequencies within any range is highly desirable to aid in evading jamming

2205 EQUIPMENT — Radio equipment varies in its vulnerability to interception and jamming The use of receivers which have the capacity for close discrimination between signals, and accurately adjusted and highly selective antennas, will minimize the effect of jamming as well as limit the range of interception by reducing the transmitter power required for reliable communication In the interest of transmission security, provision should be made for the use of such equipment insofar as possible Maintenance which improves the stability and overall performance of the equipment makes it less susceptible to jamming in general The protective features of terrain should be utilized as fully as possible in selecting the transmitting and receiving sites

2206 APPROVAL OF RADIO CIRCUITS — No circuit using radio transmission in any portion thereof should be designated as an approved circuit

2300 - WIRE TRANSMISSION SECURITY

2301 NATURE OF WIRE TRANSMISSIONS — Wire transmissions include telephone, telegraph, teletypewriter, and facsimile The conducting wire may be overhead, surface, buried, or submarine Submarine cable is less defensible than other wire lines since physical inspection of submarine cable is not practicable Interception of transmissions by induction also is much less likely to be detected on submarine cable than on land line Transmission by wire usually is less vulnerable to interception than radio or visual transmission, but wire facilities often are not available in highly mobile situations because of the advance preparation and installation required The possibilities of wire interception must be considered in communication planning and in determining the manner of use of wire circuits Wire transmissions can be intercepted by means of a direct coupling to the line or by devices utilizing the induction and radiation fields in the vicinity of the lines Skillful wire interception may be very difficult to detect In extreme forward areas, in areas previously accessible to an enemy, or where infiltration is possible, wire transmissions must be regarded as available to the opposing force Wire lines abandoned by an enemy should be used with extreme caution

a Interception by Direct Coupling — Direct coupling can be effected by direct contact with the line to be intercepted, using a metallic connection (by means of splicing wire, piercing clips, etc) Direct coupling provides interceptors a strong signal with little interference Direct coupling devices can be made quite small and inconspicuous and sensitive enough to effect interception without extracting excessive energy from the line Amplifying devices make it possible to locate and conceal a listening post, or a printing or recording device, at some distance from the point of interception

b Interception by Induction — Interception of wire transmissions can be effected even at some distance from the line, by coupling (e g , through a length of wire laid parallel to the line or a loop of wire laid flat on the ground) to that component of the electromagnetic field induced near the surface of the earth Such interception from a distance is not as satisfactory as interception by direct connection since it is subject to interference from static and other signals in the vicinity, and the interception distance varies widely in different locations It is, however, at times an effective method of interception and is usually more difficult to detect than direct coupling It must be considered in any attempt to protect the security of wire transmissions when conditions are favorable for such interception (The probability of interception by induction from conductors surrounded by a grounded metal covering (shielded cable) is negligible)

2302 APPROVED WIRE CIRCUITS

a Approving Authority — The following are authorized to issue orders or directives designating specific wire circuits as approved for the transmission in plain language of messages of a specified classification subject to careful consideration of the security aspects set forth in paragraph 2302b below

Chief of Staff, U S Army
Chief of Naval Operations
Chief of Staff, U S Air Force
Commanders of Unified Commands
Commanders of Independent Commands (when specifically designated as such by the Joint Chiefs of Staff)
Commanding Generals of Armies in the continental U S and the Military District of Washington
Commandants of Naval Districts and River Commands in the continental U S
Commanding Generals of the Major Air Commands in the continental U S
Director, Armed Forces Security Agency

b Qualifications of Approved Circuits — Preparation of an exhaustive list of specific qualifications of a circuit for approval is impossible, however, in considering the relative security of a wire circuit to determine the classification rating, the points stated below will serve as a guide

(1) Wire circuits shall not be authorized as approved circuits under the following circumstances

(a) If the circuit is located outside allied territory or is located in captured enemy territory not protected by patrols of frequent inspections

(b) If the circuit is directly accessible to hostile forces

(c) If all terminal equipment, relay stations, repeater stations, switchboards, distribution frames, etc , involved in the circuit are not maintained and operated by personnel specifically authorized by the approving authority for the security classification of material to be passed over the circuit

(d) If a submarine cable is located in waters sensitive to hostile underwater operations

(e) If the circuit employs ground return A temporary exception to this provision, based on calculated risks, is made for circuits in the continental U S and Canada However, use of circuits employing ground return is undesirable due to increased susceptibility to interception and should be avoided whenever possible

(2) Figure 1 below, does not constitute the authority for approving a circuit, but indicates the highest permissible classification rating

WIRE CIRCUIT CLASSIFICATION CHART

TYPE OF CIRCUIT	TYPE OF TRANSMISSION	TYPE OF WIRE AND LOCATION	CLASSIFICATION RATING
SPEECH	AUDIO (i e below 5 kc)	Any type of wire in terrain offering facilities for concealment of intercept equipment	UNCLASSIFIED
		Any type of wire in terrain NOT offering facilities for concealment of intercept equipment	RESTRICTED
		Physical Pair (Direct Line) Within restricted inclosure or building where the possibility of undetected interception is negligible	SECRET
	CARRIER TELEPHONY (i e above 5 kc)	Any type of wire in terrain offering facilities for concealment of intercept equipment	RESTRICTED
		Any type of wire in terrain NOT offering facilities for concealment of intercept equipment	CONFIDENTIAL
TELEGRAPHY (Teletypewriter, Facsimile, etc)	DIRECT CURRENT	Any type of wire in terrain offering facilities for concealment of intercept equipment	UNCLASSIFIED
		Any type of wire in terrain NOT offering facilities for concealment of intercept equipment	RESTRICTED
		Physical Pair (Direct Line) Within restricted inclosure or building where the possibility of undetected interception is negligible	SECRET
	VOICE FREQUENCY ON AUDIO CIRCUIT (i e below 5 kc)	Any type of wire in terrain offering facilities for concealment of intercept equipment	RESTRICTED
		Any type of wire in terrain NOT offering facilities for concealment of intercept equipment	CONFIDENTIAL
	VOICE FREQUENCY SUPERIMPOSED ON CARRIER CIRCUIT (i e , above 5 kc)	Any type of wire in terrain offering facilities for concealment of intercept equipment	CONFIDENTIAL
		Any type of wire in terrain NOT offering facilities for concealment of intercept equipment	SECRET

Figure 1

(3) Careful consideration should be given to the following factors in determining the advisability of lowering the classification rating obtained from Figure 1, above

(a) Nature of population (dense or sparse, primitive or civilized, hostile or friendly)

(b) Extent to which a line is patrolled or examined for indications of interception

(c) Extent to which repeater stations, distribution frames, terminal equipment,

etc , are guarded against unauthorized access

(d) Electrical radiation from teletypewriters (It is impossible to define exactly the maximum distances at which intelligible radiation from a teletypewriter can be received It is likely to be of the order of 2Ø to 3Ø feet, but depends largely upon the extent to which adjacent wiring might facilitate the rediffusion of signals This is important where rooms or buildings adjacent to the teletypewriter are not under Service control)

(e) Possibility of detecting interception

(f) Difficulty of disposing of information obtained (An agent obtaining intelligence by the interception of circuits in enemy territory has to dispose of his information by clandestine means This problem will vary according to the effectiveness of censorship, counterintelligence, etc)

(g) Use of former enemy or civil systems (A very careful examination of such a system should be made before approval, looking particularly for such things as unnecessary wiring on switchboards, repeater stations, and other line equipment and components, small resistors and/or condensers on terminal blocks, splices, bridges, cables, and wires leading into areas not capable of being inspected, presence of suspicious or apparently surplus equipment in the vicinity, signs of tampering with line or line equipment, etc)

c Reporting

(1) Information copies of orders or directives authorizing or rescinding the authorization of an approved circuit shall be forwarded to the appropriate authority listed below

Chief of Staff, U S Army, Attn Chief, Army Security Agency

Chief of Naval Operations, Attn Director, Naval Communications

Chief of Staff, U S Air Force, Attn Director of Communications

(2) Orders or directives authorizing an approved circuit should contain information of the following nature

(a) Geographic location

(b) Summary of requirements for the approved circuit

(c) Summary of qualifications of the approved circuit

(d) Classification rating

(e) Approving authority

EXAMPLE

Location, Tokyo, Japan
Requirements To improve the in-station handling time of high precedence classified messages between AG-message center and Communication Center crypto-room
Qualifications Circuit consists of grounded metal-covered cable lying completely within one building under U S military control which was installed especially for this purpose Cable terminates only in one switchboard at each end which provide patching to U S Army Teletypewriter TT-5/FG and associated equipment such as distributors and reperforators All terminal equipment in closed and guarded rooms which require special passes for entry which are granted only to authorized military personnel
Classification Rating Secret
Approving Authority John Q Doe, Brig Gen , USA, C Sig O, FECOM

24ØØ - VISUAL TRANSMISSION SECURITY

24Ø1 NATURE OF VISUAL TRANSMISSIONS — Visual transmissions include infra-red, flashing lights, signal flags, panels, pyrotechnics, and aircraft maneuvers Visual communication normally is more secure than radio because of its limited and predictable range Use of visual means of transmission is prescribed by commanders in consideration of the operational requirements for reliability, security, and speed of communications Visual means of transmission often can be used to eliminate radio transmissions such as receipting for messages by individual aircraft, landing and take-off communications, etc , which reveal order of battle information and are extremely vulnerable to interception and traffic analysis

24Ø2 USES

a Surface-to-Air and Ground-to-Air Communications — When practicable, surface and ground forces communicate with aircraft by flashing light, panels, and other visual methods

b Air-to-Ground and Air-to-Surface Communications — Aircraft employ maneuvers such as wing-dip, circling, etc , to communicate short prearranged messages or signals to surface and ground forces

c Ship-to-Shore and Ship-to-Ship Communications — Semaphore and flashing light are used widely in ship-to-shore and ship-to-ship communication

24Ø3 APPROVAL OF VISUAL CIRCUITS — No circuit using visual transmission in any portion thereof should be designated as an approved circuit

25ØØ - SECURITY OF OTHER MEANS OF TRANSMISSION

25Ø1 NATURE OF OTHER MEANS OF TRANSMISSION - Transmission security is synonymous with physical security in the protection of communications transmitted by messenger, mail, trained animal, etc

a Messenger and Mail — Messenger and mail are generally the most secure means of transmission and shall be used whenever time and facilities permit Such means often are more rapid than radio, visual, or wire transmission when time of encryption is considered Service regulations prescribe security requirements for preparation of such material and conditions for transmission by ships, aircraft, dispatch boat, motorized vehicles, etc The requirements for physical security vary with local conditions and are provided for by local implementation of the Service regulations

b Trained Animals — Trained animals such as pigeons and dogs have limited special use in tactical situations as supplementary means of communication

25Ø2 NON-ELECTRICAL SOUND SYSTEMS — Whistles, bugles, sirens, klaxons, small arms fire, etc , are used as a means of communicating short, prearranged messages and orders or as an alarm signal Ordinarily no special provisions are made for security of such means of communication

25Ø3 ELECTRICAL SOUND SYSTEMS — The means of communication included in this category are public address systems, inter-office communication systems, audio frequency recording systems, etc Little or no security can be ascribed to any of these systems unless they are specially designed and installed and therefore should not be used for the transmission of classified information in plain language Local commanders should establish and promulgate a policy governing the use of such systems for plain language transmission of classified information within their commands Technical assistance and advice may be obtained from local communication security units

26ØØ - SPECIAL SECURITY MEASURES

26Ø1 PURPOSE AND AUTHORITY — Communication cover and deception is a highly specialized method of providing security Generally, a cover and deception program properly employed is capable of concealing information obtainable from communications by intercept and analysis when all other techniques of communication security have failed Because a poorly conceived and executed cover and deception operation can be extremely dangerous and may jeopardize an entire military operation, not only of the employing command but also on all adjacent commands even to the entire military effort, communications cover and deception programs will be employed only in accordance with policies established by the Joint Chiefs of Staff

26Ø2 PLANNING — Cover and deception techniques require skillful and careful planning Inept attempts will result in obvious abnormalities and will invite a concentrated effort of enemy intelligence activities

26Ø3 IMPLEMENTATION — Because of the technical nature of any detailed discussion of planning for the implementation of communication cover and deception programs, as well as the classification which this material has, such material is contained in separate publications

CHAPTER 3

TRANSMISSION SECURITY IN MESSAGE DRAFTING

3ØØØ - GENERAL

3ØØ1 EFFECT OF MESSAGE DRAFTING ON TRANSMISSION SECURITY — Many of the elements of transmission which serve enemy traffic analysts as a means of producing intelligence are inherent in the drafting of messages The necessity for transmission of messages, assignment of procedence, security classification, and text of a message are accepted by communication operating personnel as presented by the originator Such factors have a vital bearing on the security of transmissions Messages must be drafted in accordance with the prescribed regulations to avoid contributing to the exposure of extensive military intelligence

3ØØ2 THE MESSAGE ORIGINATOR — The originator is the command by whose authority a message is sent The originator is responsible for the functions of the drafter and the releasing officer

a Drafter — The drafter is a person who actually composes a message for release by the originator or the releasing officer

b Releasing Officer — The releasing officer is a person who may authorize the transmission of a message for and in the name of the originator

31ØØ - ORIGINATOR'S RESPONSIBILITY FOR TRANSMISSION SECURITY

31Ø1 MINIMUM TRANSMISSION OF MESSAGES — For reasons of both security and communication efficiency, only those communications which require rapid transmission for the accomplishment of a military purpose shall be sent as messages The sending of communications by message often results in transmission by electrical means Every message so transmitted must be regarded as being available to unauthorized agents through interception and is useful to enemy traffic analysts as statistical material regardless of all security precautions which may be taken in encryption and transmission Unclassified messages transmitted by electrical means are especially damaging to transmission security since they usually are not encrypted The drafter and releasing officer should be made cognizant of the dangers resulting from indiscriminant use of unclassified messages and should be encouraged to use non-electrical means whenever time is not the decisive factor since these means preclude ready accessibility to enemy traffic analysts Much intelligence can be derived by collation of plain language messages which provide information regarding the function, activities, plans, location, morale, etc , of the station of origin and the station of address

31Ø2 BREVITY — Brevity is especially important in tactical situations when communication facilities are limited by the difficulties of wire installation and when radio transmissions, through their vulnerability to direction finding, expose unit locations When transmissions are subject to jamming, length of a transmission may be the deciding factor in receipt or non-receipt of the message, thereby aiding or hindering the maintenance of circuit discipline

31Ø3 CLARITY — Clear, concise messages prevent unnecessary queries and additional messages of explanation and the loss of security which attends such transmissions Service instructions contain details designed to achieve brevity and clarity References in message texts shall be avoided unless essential inasmuch as valuable information may be provided through linkage

31Ø4 SECURITY CLASSIFICATION — The originator is responsible for indication of proper security classification of the message in accordance with Service regulations before it is forwarded for transmission The classification governs the protective measures afforded the message in transmission and imposes restrictions on dissemination of the information contained therein

a Associated Classified Information — Adequate classification of text includes consideration of intelligence potential through inference or association with other sources of information, thus, a message sometimes requires classification apparently not justified by its textual content in order not to compromise associated information

b Message Requiring Classified Reply — A message which will inevitably require a classified reply should be classified

c Reply or Reference to Classified Message — Reply or reference to a classified message may be assigned a lower classification than the original message when the contents of the text of the message containing the reply or reference permits The rules governing the use of an unclassified message which refers to a classified message are set forth below

(1) If the original message is marked "paraphrase not required", an unclassified message quoting the date-time group and/or the originator's reference number of the subject message is permitted provided the content of the message containing the reference is itself unclassified

(2) If the original message is marked "paraphrase required", an unclassified message containing a reference to the original message is prohibited

(3) When special precautions are taken to protect address of communications (such as codress or call sign encryption), an unclassified message quoting the date-time group of a classified message protected by such procedure is prohibited This condition will be indicated by an additional warning, e g , "No unclassified reply or reference if the date-time group is quoted" on all copies of the message

31Ø5 PRECEDENCE — Since precedence determines the relative order of handling by communications personnel, it is obvious why unusually high precedences always serve to attract the attention of foreign analysts Message originators should be cognizant of the inherent danger and possible consequences of alerting the enemy with high precedences, particularly where the text of the message deals with impending operational activity

31Ø6 ADDRESSEES — Action and information addressees should be limited to those who need to know the content of the message Failure to include addressees who need to know results in transmissions detrimental to security such as services and requests for retransmissions involving re-encryptions and sometimes paraphrasing Inclusion of non-essential or unusual addressees results in the excessive use of widely held cryptographic systems and provides address patterns which imply intelligence regarding structure of the communication network and order of battle Use of book messages instead of multiple addressed messages aids in preventing the establishment of address patterns by enemy analysts

31Ø7 CANCELLATIONS — As a protective measure against imitative deception, cancellation of a message which has been transmitted will normally be given the same protection as the original message All plain language cancellations sent over nonapproved circuits should be authenticated

31Ø8 CLASSIFIED INFORMATION IN PLAIN LANGUAGE

a General — The general policy regarding the transmission of classified information is stated in paragraph 21Ø8 Instances have been reported where classification of a message has been lowered below that required by the content in order to take advantage of approved circuit facilities This practice should not be condoned

b Radiotelephone and Telephone — The policy regarding transmission security for radiotelephone and wire telephone is stated in paragraphs 41Ø3 and 42Ø2, respectively

CHAPTER 4

TRANSMISSION SECURITY IN COMMUNICATION OPERATIONS

4ØØØ - GENERAL

4ØØ1 CIRCUIT DISCIPLINE — Circuit discipline is communication operation in accordance with prescribed procedures and adherence to the principles of transmission security To minimize the information available for unauthorized analysis of traffic on any circuit, every station transmitting communications must maintain constant surveillance of its own transmissions and assure adherence to all details of authorized transmission procedures

a Joint Communication Instructions — Basic communication operating instructions, incorporating security principles, are prescribed in the Communication Instruction Series, JANAP/ACP 12Ø-139 All transmissions shall be made in accordance with the operating procedure prescribed for the particular means of transmission Procedures have been developed from experience and research to provide the most efficient and secure means of accomplishing the delivery of a message Shortcuts, elaborations, and changes to authorized communication operating procedures result in delay and confusion, encourage deception, and endanger security

b Local Communication Instructions — Local applications of joint instructions are prescribed in local standing operating procedures and local communication operation instructions They provide for the details of communication operations such as call signs, frequencies, authentication systems, communication schedules, etc , which determine many of the external characteristics of transmissions Since these details of communication operation are determined by the local operational requirements, they will reveal operational intelligence unless they are employed uniformly in accordance with local instructions which provide required security For example, if routing procedures are not employed uniformly by all stations in a net, call signs can be identified by observation of such details as relay messages transmitted on one link using a tactical call sign for address and on another link using a theater routing indicator for address Any station deviating from local authentication procedures can cause confusion throughout the net, invite enemy deception, and establish a continuing identification of itself by such characteristic operation

4ØØ2 MINIMUM TRANSMISSION BY ELECTRICAL MEANS — Electrical transmissions shall be minimal Only information which requires electrical transmission in order to accomplish a military purpose shall be transmitted over electrical circuits Messenger, mail, or other means of transmission shall be used whenever necessary communications can be so accomplished Those messages which require electrical transmission shall be as brief as possible

a Prosigns and Operating Signals — Prosigns and operating signals shall be used only as authorized When properly used, prosigns and operating signals expedite message handling They must be considered the equivalent of plain language and must be employed with discretion Security requirements in the use of operating signals and prosigns vary with the military situation and depend upon the apt application of basic security principles

b Services — Service messages and procedure messages should be kept to a minimum by using authorized procedures for transmission, by checking encipherment before transmission, by the use of garble tables to correct faulty transmission received, and by attempting to determine errors in encipherment before servicing, when time permits The linkage between messages provided by services is extremely helpful to enemy analysts in determining the continuity of encrypted call signs and transmission schedules and in cryptanalysis

c Unofficial Transmissions — Unofficial transmissions or personal conversations increase vulnerability to interception, encourage imitative deception, and provide traffic analysts a great volume of personal data which can be used for identification purposes and which often has intelligence value when related to other information Unofficial conversations must be eliminated to prevent the fragmentary disclosure of detailed information regarding identity of units, strength, morale, supply, equipment, state of training, organization and operation of the communications network, suggestion of geographical location through reference to weather or local conditions, and amplifying information regarding any element of transmission

4ØØ3 TRANSMISSION OF CLASSIFIED INFORMATION IN PLAIN LANGUAGE

a Over Approved Circuits — When approved circuits are available, adherence to the

following requirements in communication operation will decrease the risk incurred in establishing the approved circuit

(1) Maximum use of existing crypto-facilities should be made in preference to using an approved circuit

(2) A classified message which will require relaying to reach the addressee(s) may be transmitted in plain language over an approved circuit only when it can be determined that the addressee(s) will be reached solely by approved circuits of adequate classification rating If there is any possibility that alternate routing may result in the transmission of the message by means other than an approved circuit of adequate classification rating, the message requires encryption by the station of origin, except as provided in paragraph 21Ø8

(3) The security classification of messages transmitted in plain language over approved circuits shall be transmitted as the first work of the text

b Over Nonapproved Circuits

(1) Classified information will not be sent in plain language over nonapproved circuits except as provided in paragraph 21Ø8 Each such message authorized for transmission in plain language shall be identified by the phrase "SEND IN CLEAR" signed by the Commanding Officer or his specifically authorized representative

(2) Classified messages sent in plain language over nonapproved circuits shall be identified as such by the inclusion of the word 'CLEAR" as the first word of the text and will be handled in accordance with the actual security classification, if known, otherwise, it will be handled as CONFIDENTIAL security information

(3) A classified message received in the clear over a nonapproved circuit will be marked "CLEAR" or "RECEIVED IN CLEAR" and will be handled as CONFIDENTIAL security information Should the addressee desire to forward the information, a new message shall be originated, handled, and transmitted as appropriate The original message shall in no case be readdressed

(4) Extreme care will be exercised in transmitting messages in plain language not to indicate the contents (addressee(s), subject matter, etc) of previously encrypted messages, nor will any information about cryptonets or references to systems held or not held by a station be transmitted in plain language over a nonapproved circuit except as provided in paragraph 21Ø8

4ØØ4 CALL SIGNS, ROUTING INDICATORS, AND ADDRESSING INFORMATION

a General — Determination of the general requirements for call sign security and the means to be employed in achieving the required protection is a responsibility of communication planning, and general provisions for security are incorporated in communication operating instructions This is discussed in detail in Chapter 2 Whatever the means employed, the manner of application is of utmost importance in ultimate achievement of security Consequently, communication operating personnel must be trained to recognize and avoid practices which lead to compromise of call sign and addressing information for which protection is required

b Sources of Compromise — Call sign compromises may occur in an unpredictable number of ways The principal contributing sources include the following

(1) Physical Loss or Capture of Call Sign Documents and Assignments — The physical protection required for call sign assignments is governed largely by proper classification Although call sign assignments contained in classified publications sometimes may be individually unclassified, subordinate commands frequently do not have sufficient information to determine the proper classification of individual assignments Accordingly, in the absence of explicit instructions to the contrary, specific call sign assignments shall be given the same classification as the publication from which extracted, and protection shall be commensurate with that classification

(2) Plain Language Disclosures in Transmission — Plain language disclosures constitute one of the most serious sources of compromise Most frequently occurring violations are promulgation of call sign assignments by plain language message and disclosures of unit identities and call sign assignments in unauthorized operator chatter Other types of plain language disclosures are discussed in paragraph 4Ø4 b(3) below

(3) Linkage of Protected Call Signs with their Plain Language or Unprotected Equivalents, or with Variants of the Same Call Sign — Any transmission which directly or indirectly links call signs or addressing information on that transmission to different call signs or address designations on prior or subsequent transmissions provides a potential threat to the security of message headings Linkage cannot be completely avoided, but training of operators to recognize the factors which constitute linkage will reduce the extensiveness of linkage and contribute to desired security Specific malpractices, usually resulting in undesirable linkage, which must be avoided to the maximum practicable extent include

(a) Use of a call sign or address designator together with its plain language equivalent in the same message heading

(b) Use of superseded call signs, particularly when call signs are changed daily or at frequent intervals to provide security This practice establishes linkage between the old call sign which may have been identified by the enemy, and the new call sign

(c) Use of protected call signs and unprotected call signs (or plain language designations) in successive transmissions A station originating a transmission using an encrypted or otherwise protected call sign, and following it immediately with a transmission using unprotected call signs, has obviously lost any security afforded by the protected call sign

(d) Conversion of protected calling and addressing information to unprotected or plain language calling in relaying, retransmitting, or readdressing a message without otherwise altering the original message, and vice versa

(e) Making reference in plain language services to a message of the previous day when encryption or daily change is used to provide call sign security

(f) Use of protected call signs or addressing information on plain language messages when the content of the message discloses the identity of the originator and/or addressee

(g) Use of protected call signs in the call-up and synonymous unprotected designations in the address portion of a message, and vice versa

(h) In multiple address messages, address patterns are frequently established with the result that protected addressees sometimes are identifiable by their association in the same message with other addressees From a practical standpoint this may be unavoidable at times In some cases, particularly when various addressees are reached over different circuits, use of separate transmissions is more secure since the enemy will be required to intercept each message in order to reconstruct the address pattern

(4) Collateral Information — Call signs may be compromised by information available from sources other than communications For example, when the location of a particular activity in a given area is known to the enemy through prisoner-of-war reports, intelligence reports, or captured documents, transmissions originating from that location may be pinpointed by direction finding, and if a protected call sign is used it may be identified in this manner This type of identification may be of great value to enemy analysts in reconstructing other call sign assignments, particularly in the event that assignments are systematic There is little that can be done by communication operating personnel to provide protection specifically against this type of compromise

c Other Insecure Practices — Some other practices which do not necessarily result in specific call sign compromises, but which weaken methods employed to provide call sign protection, are described below

(1) Peacetime use of variants which are assigned and reserved for use only when encryption is ordered in effect may weaken the security of the call sign cipher

(2) Failure to use prescribed variants may result in weakening the security of the call sign cipher

(3) Local expansion of tactical call signs (by suffixing or prefixing) according to a fixed organizational pattern provides the enemy with a key to internal communication organization

(4) Use of station or message serial numbers in conjunction with indefinite call signs designed to protect the identity of a mobile communication station may result in the ultimate identification of call signs and communication station, since serial numbers provide a basis for sorting traffic by individual originators

(5) Use of plain language addressing information on encrypted messages, although sometimes unavoidable, is detrimental to security since enemy analysts may establish subsequent linkage with protected addressing information Its use also may be of great value to cryptanalysis in permitting assumptions of textual content

(6) Failure to arrange in alphabetical order, after encryption, encrypted calls appearing in the address portion of multiple address messages may result in identifications through linkage with previously established multiple address patterns

4005 DEFENSE AGAINST IMITATIVE DECEPTION — Defense against imitative deception depends upon the following factors

a Circuit Discipline — Adherence to authorized operating procedures and observance of transmission security regulations is important to the prevention of imitative deception Enemy transmissions are conspicuous in a net in which circuit discipline is maintained constantly When deception can be recognized by incorrect operating procedures or flagrant violations of security regulations, deception can be evaded or countermeasures can be taken On the other hand, operator chatter, failure to authenticate and failure to observe operating procedures invite imitative deception which is likely to succeed under such circumstances The enemy's ignorance of operating details is not conspicuous on poorly disciplined circuits, whereas it might betray the deception on well-disciplined circuits

b Alert Operation — Alertness of operators is necessary to detect incongruities which indicate imitative deception Some of the most common techniques employed in imitative deception are

(1) Answering calls and accepting traffic when the called station fails to reply promptly

(2) Receipting for messages which the intended addressee has not been able to copy accurately or completely

(3) Calling and pretending to have important traffic or interrupting transmissions of high precedence to send a higher precedence

(4) 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 circuit

(5) Originating and transmitting false plain-language messages

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

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

(8) Imitating irregularities in procedure and characteristics of tone or keying

c Use of D/F — Direction-finding on suspected transmissions provides a check on the origin of transmissions

d Authentication — Authentication is the verification of transmissions or stations as bona fide

(1) The usual method of authentication is the transmission of prearranged signals When authentication systems are not prescribed for general use by the Service, they are formulated locally in accordance with joint instructions set forth in AFSAG 1247, and are authorized for joint or intra-Service use Specific directions for authentication to meet the operational requirements are incorporated in operating instructions which provide for the authentication of individual stations, mutual authentication of two or more stations (by challenge and reply) and authentication of transmissions

(2) Authentication should be required in 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 completing authentication

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

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

(e) When transmitting a plain-language cancellation over a nonapproved circuit

(f) When transmitting plain language operating instructions which affect the military situation Example Closing down a station or watch, shifting frequency, directing establishment of a special guard

(g) When making initial radio contact Authenticators should be exchanged to prevent an unauthorized station from establishing contact by asking a legitimate station to authenticate

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

(3) Authentication may also be required under other circumstances by local commanders

(4) Procedure for authentication and procedure for transmission of authentication are specified in operating instructions for specific authentication systems and may be incorporated in local communications operating instructions

(5) Readiness to authenticate and accuracy in authentication are of the utmost importance It is therefore necessary that authentication be used sufficiently often in training to insure that all personnel concerned are thoroughly trained To this end it is desirable that all stations be required to authenticate occasionally Additional intensive training within each station is also desirable

41ØØ - SECURITY OF RADIO TRANSMISSION

41Ø1 GENERAL

a Defense Against Enemy Direction Finding — In tactical situations, when concealment of the identity and location of military elements is highly desirable, defense against interception and direction finding is an important consideration in communication operations A transmission of very short duration may be sufficient to permit bearings to be taken Simultaneous bearings from different locations make possible the plotting of the source of transmission and topographic limitations may make possible determination of a transmitter's position from even a single bearing When transmissions are extensive, very accurate plotting of the source of transmission is possible

(1) By determining the origin of transmissions, intercept operations are aided in determining the identity of radio stations regardless of changes in frequency, time of transmission, call signs, number series, etc The value of such intelligence to an enemy makes it imperative that radio transmissions be reduced to the absolute minimum in tactical situations

(2) When protection of the location of a transmitter is highly desirable and radio transmission is necessary, it sometimes is feasible to accomplish the transmission from a different location Submarines may withdraw from station to transmit essential information by radio, aircraft may be sent some distance from the protected location to transmit important traffic, or the traffic may be sent by wire or courier to another station for transmission

(3) High standards of frequency adjustment aid indirectly in protection against enemy direction finding by reducing the number of transmissions required to establish and maintain communications

b Radio Silence — Radio silence must be rigidly observed when ordered

(1) Conditions of radio silence are specified by commanding officers to meet strategic or tactical requirements The convenience and speed of radio communication are not sacrificed voluntarily by a commander unless the need for silence is extremely important If radio silence is broken the new positions can be located by direction-finders, tactical plans can be predicted, and the use of other protective devices is sacrificed needlessly

(2) It is permissible to break radio silence in extreme situations such as enemy contact or the enemy's discovery of a unit's position or when the transmission of information regarding the operation becomes more important than the concealment of location and the intelligence which could be derived by the enemy Service regulations provide for exceptions to the restrictions of radio silence for lost planes, for Naval and Air elements upon encountering hazardous weather, etc

(3) When it is necessary to break radio silence to accomplish essential communication, radio silence should be resumed immediately upon completion of the exceptional communication, and maintained as directed or until the condition of radio silence is terminated by competent authority

c Anti-Jamming Techniques — Operator training is the most effective defense against jamming An operator must be able to recognize jamming, be aware of means to cope with the particular type of jamming, and deny the enemy any opportunity of determining the effectiveness of the jamming Training and continued practice are required to develop proficiency in operating while subjected to jamming

(1) The widely varied types of jamming must be familiar to the operator if he is not to be disconcerted and diverted from effective operation Through training and continuous practice an operator can learn to recognize jamming and to work through interference Jamming-signal generators and recordings are effective training aids

(2) Thorough familiarity with anti-jamming devices and the controls of receiving equipment is necessary in order to realize the capabilities of adjustment which often make effective communication possible through jamming

(a) Increase of transmitting power often will offset jamming enough to make the desired signal readable

(b) Accurate adjustment of transmitters and receivers to the required frequency will avoid the impaired signal from off-frequency operation which increases vulnerability to jamming

(c) Operators familiar with automatic jamming can evade it by stopping transmission until the jamming is automatically transferred to another frequency, then resuming transmission until the jammer returns to the frequency

(d) It may be possible to evade jamming by alternate routing

(e) Simultaneous keying on two frequencies with "split-phone" circuit coverage will make it possible to evade jamming, or require the expenditure of greatly increased effort by the enemy

(f) Anti-jamming techniques vary with the circumstances They can be developed to a high degree by experience and training Experienced operators, taking full advantage of all means available to receive the desired signal, can make it necessary for an enemy to use greatly increased power to achieve the desired jamming effect, and the increase is sometimes difficult or impossible to attain

(3) Observance of security regulations and adherence to operating procedures minimizes opportunities for jamming by denying unauthorized agents knowledge of communication operations, which is necessary for effective jamming

(4) All details of jamming should be reported to appropriate authority in order that effective countermeasures may be taken Jamming signals should be located by use of D/F when such equipment is available Reporting procedures are specified in Service instructions

d Net Discipline — All directives of the net control station shall be strictly observed by stations within the net Compliance with the net control station's orders is essential to effective and secure communications

(1) In tactical situations, operating conditions may require the limitation of transmission to messages of high precedence only, or may require that permission be obtained from the net control station before transmitting to another station in the net The net control station will direct such operation as is required by the situation

(2) Stations will not leave a net to communicate with stations in a different net except in extreme emergencies and then only with the permission of both net control stations Normally, traffic for a station in another net will be relayed through the net control stations of the two nets

e Radio Watches — The manner in which a radio watch is maintained bears on the achievement of transmission security in that alert operation, meeting of schedules, and operating on correct frequencies aid in avoiding excessive transmissions, thereby reducing vulnerability to interception and direction finding Failure or delay in answering a properly authenticated call invites enemy deception in the form of receipting for traffic and thereby quieting the transmitting station's attempt to deliver the communication to the intended addressees

f Equipment Adjustment — Combinations of transmitters, antennas, and power should be such that the minimum wave propagation and emission intensity consistent with reliable communications is used Any increase in range of transmission increases the range of interception

(1) No station should transmit other than the type of emissions authorized or on other than the frequencies authorized

(2) Transmitters and receivers must be adjusted to conform to local and Service specifications regarding frequency and power tolerance limits Provision should be made for continuous check maintenance as improper adjustment of transmitters and

receivers results in failure to establish communications and excessive transmissions, thereby increasing the opportunity for interception, direction finding, and jamming

(3) Emissions incidental to testing, tuning, changing frequency, and adjustment of equipment must be reduced to the absolute minimum Transmissions of any kind provide an opportunity for direction-finding activities to get bearings on the transmitter Whenever the necessary equipment is available, radio transmitters shall be tuned on a secondary equivalent ("dummy) antenna from which there is no emission Tuning transmitters with radiating antenna connected alerts intercept, enables D/F stations to take bearings, and interferes with adjacent frequencies

(4) When frequencies are shifted to evade interception, success greatly depends upon concealment of the frequency shift in communications operations Clear-text transmissions must avoid any reference to changes in frequency to avoid alerting intercept If possible, operators should be shifted when frequency and call sign are changed

g Requests and Reports Concerning Readability — Requests and reports concerning signal strength and readability shall be transmitted only when necessary to establish communications

h Characteristic Transmissions — All characteristic transmissions are to be avoided in order to deny enemy traffic analysts that means of establishing identity and assuring continuity of interception

(1) Transmitters can be identified through characteristics as shown on an oscilloscope and recorded on film, or an experienced intercept operator often can recognize a transmitter by sound alone An identifiable transmitter which has been associated with a particular call sign or frequency can be used to identify a station after the call sign has changed, or sometimes when transmitting on a different frequency, and thus lead to solution of the method of communications operation

(2) Operators should not identify themselves by transmitting personal signs or names of any kind, or by transmitting with a recognizable rhythm or personal variation in operating procedure If an operator can be identified, his unit will be recognizable through his operating in spite of encrypted call signs, changing frequencies, and other protective measures

(3) Functional differences in communication traffic result in characteristic traffic patterns in which volume, precedence, message length, time of transmission, etc , differentiate supply, operational, or administrative traffic Military activities are reflected in the traffic pattern by fluctuations in volume, classification, and precedence of messages

(a) Long encrypted messages may be detrimental to security when they can be associated with operational activities, when they are indicative of impending operational activity, or when their recurrent nature makes them characteristic of the originator and addressee and therefore a means of identifying units or confirming assumptions For example, if a headquarters transmits regularly an exceptionally long message to the same addressee, that message alone may provide a means of tracing the headquarters when moved or may be indicative of the extent of activity at the headquarters, since it is practically certain to be a recurring report of a specific nature When it becomes necessary to provide protection for such information, a simple protective measure is the division of the message into several shorter messages which do not exceed average message length established for that headquarters, and which are prepared in such a manner as to appear unrelated externally More specific instructions are contained in AFSAG 121Ø, Cryptographic Operations — Joint

(b) When the concealment of routine reports and stereotyped messages is necessary to prevent the identification of stations and links through recognizable transmissions, the external appearance and time of transmission should be varied insofar as possible consistent with operational requirements

41Ø2 RADIOTELEGRAPH

a Broadcast and Intercept Methods of Transmission — Broadcast or intercept method of transmission should be used in preference to receipt method whenever possible The silence of receiving stations increases transmission security greatly By these methods radio stations can receive traffic without incurring the risk of direction-finding operations against them The broadcast method provides for transmission of traffic to be copied by specified stations according to prearranged schedule and without acknowledgement The intercept method provides for transmission of traffic between two stations which acknowledge receipt of traffic, request repetitions and corrections, while a third station or other stations copy the traffic which actually is intended for them

b Speed of Transmission — Transmissions should be made at a copyable speed and speed keys shall be used only by qualified speed key operators when specifically authorized by competent authority Unless all operators in a net are capable of sending and receiving at high speeds, such transmissions result in inaccuracies and the use of excessive circuit time in requesting and giving corrections and repetitions, with consequent impairment of security through unnecessary transmissions and increased opportunity for intercept

41Ø3 RADIOTELEPHONE — Experience has shown that use of radiotelephone by other than trained personnel often results in delays, misunderstanding, and loss of security, which defeat the purpose of communication Correct use of equipment and adherence to operating procedures are essential for the most effective use of radiotelephone All personnel using radiotelephone facilities shall be informed of the security risks of enemy traffic analysts and direction finding to which such transmission is subject Since no definitive security can be provided for plain language radio transmissions, they must be considered as available to the enemy

a Use — Each circuit must be used for its intended purpose only, and a minimum number of transmissions shall be made Circuits used for unauthorized transmissions are not available for the intended purpose when needed

b Preparation of Messages — Whenever possible, contents and wording of a message should be considered before starting the transmissions In the interest of clarity, brevity, and security, messages should be written before transmission whenever practicable

c Nature of Transmissions — Transmissions must be concise and clear

d Classified Information — Classified information must not be transmitted in plain language except as provided in paragraph 21Ø8 Unauthorized plain language reference must not be made to classified titles, units, places, charts, maps, or persons in such a way that the nature of the headquarters, task force, or other unit concerned will be revealed, nor shall veiled language be used to express classified information It gives the user a false sense of security, may confuse the intended listener, and cannot be regarded as any more secure than direct statement

e Incidental Transmissions — Radiotelephone transmissions must be protected from classified conversation or interfering noise in the background

f Call Signs — Radiotelephone call signs must not be linked to other call signs

g Operating Procedures — Radiotelephone operating procedures must be observed at all times

41Ø4 RADIOTELETYPE — All the provisions of paragraph 41Ø1 apply to radioteletype transmission There is a tendency to regard the more complex communication equipment as more secure than radiotelephone and radiotelegraph There is no basis for such a supposition Radioteletype transmissions are equally vulnerable to interception even though added effort is required for the interception Intercepted radioteletype transmissions may, in fact, provide more accurate intercepted copy than radiotelephone or radiotelegraph transmissions

42ØØ - SECURITY OF WIRE TRANSMISSION

42Ø1 GENERAL — In addition to the general provisions of transmission security in Section 4ØØØ, the physical security of the wire lines must be regarded as an element of transmission security for wire circuits, particularly when the conditions for successful intercept become favorable When the danger of interception is great, wire lines should be policed by personnel who have been familiarized to recognize evidences of interception

42Ø2 TELEPHONE — The provisions of paragraph 41Ø3 a - e concerning the use of radiotelephone apply as well to the use of telephone on wire circuits Operators should be alert for unnecessary sounds such as are made by making and breaking direct metallic contact with the circuit

43ØØ - SECURITY OF VISUAL TRANSMISSION

43Ø1 GENERAL — Visual transmission security depends upon prevailing conditions of visibility and proximity of the enemy Protection of visual transmissions, therefore, is concerned with limiting the range of visual transmissions to the minimum necessary for effective communications, and restriction of visual transmission, insofar as consistent with operational requirements, to times when it cannot be intercepted without the knowledge of the sender Visual means is normally more secure than radio, since the range is more limited and the directivity more controllable

43Ø2 VISUAL METHODS — The visual methods employed in military communications in relative order of security are as follows

a Infra-Red (Nancy) Infra-red is a system of communication utilizing light outside the visible spectrum to transmit International Morse Code characters It necessitates the use of special equipment and affords greater security than other visual means Nancy equipment can be used when visual communication is necessary and visual silence has not been prescribed It is the most secure method of visual communication

b Hand Flags — Hand flags are visual means of communication involving the use of one or two flags held in the operator's hands

(1) Semaphore is a system of visual communications wherein transmission is accomplished by the use of two hand flags, the relative positions of which represent letters of the alphabet

(2) Wig-wag is a visual system of communication wherein motions of a single hand flag to the right or left are used to represent the dots and dashes of the International Morse Code In wig-wag it is necessary to know the direction in which the operator is facing, but given this information it has an advantage in that the operator may remain concealed

(3) Morse flag is a system of communication wherein the movement of a single hand flag through an angle of 9Ø or 18Ø degrees represents dots and dashes of the International Morse Code This method does not allow concealment of the operator

c Directional Flashing Light — Directional flashing light is a system of communication employing a light confined to a narrow beam to transmit International Morse Code characters This includes the blinker tube and the high power signaling searchlight Directional flashing light provides some security, owing to its directional characteristics, by reducing the possibilities of interception, however, simultaneous transmission to several stations is possible only when the bearings of the receiving stations from the transmitting station are very close together The aperture of flashing light equipment should be kept as narrow as practicable at all times If it is necessary to use flashing light during morning or evening twilight, lights should be dimmed with suitable filter and conical adapter

d Panels — Panels are visual means of communication wherein specially designed shapes are arranged in accordance with a prearranged code to convey short messages for recognition purposes They are used between air and ground or air and surface units

e Flaghoist — Flaghoist is a visual system of communication utilizing flags and pennants It is limited to the transmission of signals from signal halyards assigned for the purpose and is employed by ships and between ships and shore stations Flaghoist is limited to daylight use and to comparatively short distances

f Pyrotechnics — Pyrotechnics are those visual means of communication utilizing flares, rockets, and smoke They are employed for prearranged signals or for recognition purposes Pyrotechnic codes used for warning, recognition, marking locations, mission accomplished, requests for reenforcements or supplies, etc should be changed frequently to maintain security

g Non-Directional Flashing Light — Non-directional flashing light is a system of communication employing a light to transmit International Morse Code characters in all directions This system includes the yardarm blinker, a signal searchlight used at night, and Special All-Round Daylight Signalling Equipment (DSL) Non-directional transmission permits simultaneous delivery

to stations in any direction, but has little security from interception, particularly at night

4303 VISUAL SILENCE — Visual silence requires that no type of visual means be used Violation of visual silence is justified only in extreme circumstances when the necessity for communication is more important than the concealment of presence In such cases, the most secure visual means available should be used Prescribed visual silence should be resumed immediately after accomplishment of necessary communications

4304 MONITORING OF VISUAL CIRCUITS — Visual circuits should be monitored locally to improve security

44ØØ - REPORTING TRANSMISSION SECURITY VIOLATIONS

44Ø1 GENERAL —Departures from authorized communication operating instructions is detrimental to transmission security, but some violations of transmission security are of more immediate consequence than others Transmission security requires the reporting of those violations which in themselves specifically constitute a possible compromise of classified information All communication operating personnel should be alerted to recognize, and report to their immediate superiors, serious transmission security malpractices by stations and commands with which they are in communication, since it is patently impracticable for security monitoring and analysis activities to maintain complete surveillance of all communications The communication or signal officer of the detecting command shall determine the necessity for forwarding such reports Information contained in this section is provided for guidance in making such determination and subsequent reporting Chapter 5 contains instructions relative to reporting by communication security monitoring activities

44Ø2 POSSIBLE DISCLOSURES OF CLASSIFIED INFORMATION — Any transmission which in itself makes classified information immediately available to unauthorized intercept activities requires immediate reporting if, in the opinion of the reporting authority, serious consequences may result The military disadvantage resulting from communication compromises of classified information can be countered only if such compromises are recognized and reported immediately

a Nature of Violations — The seriousness of transmission security violations will vary with the operational situation Communication operating personnel must understand the principles of transmission security and their application to a local situation as indicated in local instructions It is impossible to describe herein all malpractices which should be reported The following examples of more frequent violations of transmission security are likely to be of a serious enough nature to require reporting and are furnished as a guide in reporting

(1) Examples of violations which almost inevitably compromise classified information are

(a) Transmission of classified information in plain language on nonapproved circuits or on approved circuits of inadequate classification

(b) Plain language disclosure of protected call sign and address group assignments or linkage between protected and unprotected call signs

(2) Examples of violations which may contribute directly or indirectly to compromise of classified information depending on the circumstances of transmission are

(a) Violation of communication silence when communication silence has been imposed to conceal information concerning the location or presence of units or activities

(b) Unofficial transmissions and operator chatter

(c) Transmission of operator's name or personal sign

(d) Excessive transmissions When the location of a transmitter is classified information, that information may be compromised by unnecessary transmissions which facilitate enemy intelligence operations and subsequent determination of the transmitter location

b Content of Transmission Security Violation Reports — Reports of transmission security violations should include sufficient information to assist in assessing the seriousness of the violation Such information might include a description of the violation, identification of the transmission, identification of the circuit on which transmitted, reference to the authority for procedure violated, and such other information as considered necessary, or required by Service instructions

c Addressing Transmission Security Violation Reports — Transmission security violation reports should be forwarded in accordance with the appropriate instruction as follows

(1) When the reporting command is of the same Service as the command being reported

an action copy should be forwarded to the command responsible for the occurrence of the violation Information copies should be forwarded to other Service commands concerned as required by Service instructions, and to one of the following as appropriate

Chief, Army Security Agency (GAS-5Ø), Washington, D C
Director, Naval Communications (Op-2Ø2), Washington 25, D C
Commanding General, U S Air Force Security Service (STD),
Brooks Air Force Base, Texas

(2) When the reporting command is of a Service other than that of the command being reported, and liaison between elements of different Services has been authorized for local reciprocal exchange of reports, an action copy should be forwarded to the command responsible for the occurrence of the violation Information copies should be forwarded to the Service cryptologic agency of the reporting command as listed in (1) above for forwarding as appropriate

(3) When the reporting command is of a Service other than that of the command being reported and liaison between elements of different Services has not been properly authorized, an action copy should be forwarded to the Service cryptologic agency of the reporting command as listed in (1) above for forwarding as appropriate

d Action Upon Receipt of Transmission Security Violation Report

(1) The command responsible for the violation will take such remedial or corrective action as the operational situation warrants

(2) Other addressees will consider the reported violation in the light of other pertinent data affecting transmission security and take such action as deemed appropriate

44Ø3 PROCEDURAL MALPRACTICES — There are procedural malpractices which do not in themselves make classified information immediately available but, when used in conjunction with other malpractices on the same or related communication circuits and information from other sources, provide the means for deriving classified information Such malpractices may not require individual reporting, however, they must be corrected in the interest of improving circuit discipline thereby improving transmission security The extent to which classified information is compromised by procedure discrepancies is primarily determined by monitoring and analysis, and the compilations of discrepancies may be summarized in procedure discrepancy reports to the responsible command

CHAPTER 5

SECURITY MONITORING AND ANALYSIS

5ØØØ - GENERAL

5ØØ1 INTRODUCTION — The contents of this chapter provide a guide for organizations, activities, and units which have security monitoring and analysis as a primary function Monitoring performed by net control stations in the interests of maintenance of security is subject to the principles set forth in Chapter Four

5ØØ2 DEFINITION — Security monitoring and analysis is the obtaining and examining of friendly communication transmissions in the interest of improvement of overall communication security

5ØØ3 FUNCTION OF COMMAND — Service cryptologic agencies (Army Security Agency, Naval Security Group, and U S Air Force Security Service) provide personnel technically trained and equipped to perform security monitoring and analysis at the request of command, as a technical service to command Monitoring by Service cryptologic agencies and supporting units or activities provides a check on monitoring by net control stations, but is not a substitute

a Means

(1) Army Security Agency — Army Security Agency provides security monitoring and analysis personnel organized and equipped to meet the operational requirements of the command which they support

(2) Naval Security Group — Communication security activities of the Naval Security Group provide communication security monitoring and related functions for Naval activities in the areas where such Security Activities are located

(3) U S Air Force Security Service — The U S Air Force Security Service provides security monitoring and analysis service for Air Force Commands through security squadrons and detachments geographically located to provide communications coverage for requiring Air Force commands The Air Force Security Service provides an additional service through its "Communications Security Improvement Teams (CSIT) A team can be made available to any command or theater for the purpose of making surveys of any communications facility On-the-spot examination is made of the security of operating procedures and message preparation and handling practices Each team is composed of an officer and non-commissioned officers of the first three grades who are highly skilled and capable of making thorough examinations and logical recommendations for security improvement

b Objectives — The objectives of transmission security monitoring and analysis performed as a service to command are

(1) To determine what effect the traffic analysis of communications by an enemy might have on the enemy's activities, and to enable the commander to determine what revision of the tactical evaluation is necessary as a result of the intelligence available to the enemy through traffic analysis

(2) To determine what deviations from communication operating procedures and what violations of transmission security are prevelant Transmission security monitoring and analysis serve to indicate what corrective measures are necessary to fulfill the commander's responsibility for implementation of existing policies and procedures affecting transmission security

5ØØ4 FUNCTION OF EVALUATING AGENCIES

a Service Cryptologic Agencies — The Service cryptologic agencies perform security monitoring and analysis at their headquarters and through their field stations on a world-wide intra-service basis in fulfillment of the responsibility for evaluation of the effectiveness of communication operating procedures and transmission security measures within each Service

b Armed Forces Security Agency — Armed Forces Security Agency evaluates monitoring, collates and performs analysis on a world-wide, joint basis in fulfillment of Armed Forces Security Agency's responsibility for the formulation of joint transmission security policy, doctrine and techniques

c Objectives — The objectives of security monitoring and analysis performed as a function of evaluating agencies are

(1) To determine what revisions of existing communication policies and procedures are necessary to facilitate communications and enhance transmission security

(2) To determine what traffic control is needed to provide communication security in support of military operations and to provide the detailed data regarding circuit characteristics which are necessary for effective traffic manipulation

51ØØ - OBTAINING TRAFFIC

51Ø1 GENERAL — The principle method of obtaining material required for the security analysis performed by evaluating agencies is obtained through "patching-in" to teletype circuits, actual interception by the appropriate Service monitoring unit or activity, and requesting material from communication centers

51Ø2 METHOD — The method of obtaining traffic and the type of equipment used will depend upon the type of circuits to be monitored, volume of traffic, distances involved, type of equipment available and state of training of security monitoring personnel Requirements for each mission will be determined by the local situation

a Teletype — Much military traffic is carried by teletype and an increasing volume of this type of traffic is indicated by expanding tape relay facilities Teletype traffic for security monitoring is obtained by the following methods

(1) The simplest method of obtaining teletype traffic is by means of connecting teletype receiving equipment to the circuit under surveillance through a switchboard This method (patch-in) provides complete monitor copy with a minimum of personnel and equipment

(2) Teletype traffic may be obtained for security monitoring purposes by arrangement with the signal centers of the monitored units to provide copies of all messages sent and received A disadvantage of this method is that it does not provide a complete copy of a circuit since service messages, chatter, test copy, etc , which are potential sources of impaired security, are not included in signal center copy

(3) Actual interception of the transmitted signal is the least desirable means of obtaining teletype traffic for monitoring since it requires highly skilled technicians and the use of expensive bulky equipment

b Telegraphy and Telephony — Since most tactical commanders of Naval and Air elements and lower echelon Army elements must rely on telegraphy and telephony circuits, the security of such circuits is of vital and immediate importance

(1) Actual interception of the transmitted signal is considered the only satisfactory method of monitoring radiotelegraph and radiotelephone circuits Communication instructions of the units concerned provide monitoring personnel with necessary information regarding frequencies and schedules of operation

(2) Patch-in at a terminal switchboard is the method used to monitor telephone and telegraph wire circuits

51Ø3 MONITORING EQUIPMENT — Equipment necessary for conduct of security monitoring is incorporated in the monitoring units' tables of allowances or tables of organization and equipment which are prepared by the Service security headquarters Specific equipment requirements will vary with each type organization which has been formed to perform a specific operation

51Ø4 RECORDING EQUIPMENT — Recording equipment is used to the fullest extent practicable in monitoring telephone and telegraph circuits, since it combines the advantages of accuracy and efficiency Voice transmission often is extremely difficult to transcribe because of variations in the rate of transmission, but repeated play-backs of a recording make accurate monitor copy possible Recording equipment also minimizes errors resulting from the pressure of copying manual traffic directly Operational personnel are employed more efficiently when one operator can record several circuits simultaneously and accurate transcription can be made at a later time Recording may be accomplished by tape, belt, wire or disc recorders Selection of the proper equipment for recording will depend to a great extent upon the specific mission and a consideration of the advantages of the recording devices

a For recording telegraph and semi-automatic Morse transmissions, a paper tape recorder usually is most feasible since it provides a permanent visual record of the monitored transmission

b For telephone circuits, the types of equipment in most common use are magnetic tape and plastic-belt type recorders and reproducers The plastic belt type of equipment has many disadvantages, including inefficient use of belts, lack of high fidelity and occurrence of creases in plastic belts It provides a permanent record of the transmission, however, and is more economical to operate than wire or disc-type records Magnetic tape is also economical and records with high fidelity

52ØØ - METHODS AND TECHNIQUES OF ANALYSIS

52Ø1 GENERAL — Since the purpose of security analysis is to determine what security prevails in communications and what measures are required to deny the enemy intelligence which could be derived from traffic analysis, the method of analysis will vary with each situation This section is not intended to be a detailed and exhaustive treatment of security analysis methods and techniques but is limited to a general discussion of the necessary steps involved in processing traffic for analysis and the basic requirements for all transmission security analysis Security analysts examine traffic from the enemy's point of view, attempting to produce intelligence through close observation of details, through inference, deduction, and the perception of relationships The formulation of a detailed procedure for traffic analysis which would be applicable in every situation is not possible The method of analysis depends upon the resourcefulness and ingenuity of analysts in studying situations which vary widely and change constantly Any technique which might be used by the enemy for extracting intelligence from communications can be applied to the monitored traffic to determine what protective measures need to be taken

52Ø2 PROCESSING — A systematic means of recording and tabulation may be required to accomplish the processing of monitored copy accurately and efficiently Expedient record and register forms are formulated, as determined by the nature of the mission, to record such information as identification of monitored traffic (by station, net, frequency, call sign, etc), number of messages received, date received, personnel responsible for different phases of processing, etc Provision can be made also for the recording of any special data needed for statistical studies

52Ø3 DERIVATION OF INFORMATION — Traffic is examined closely for any item which might lead to the production of intelligence Fragmentary disclosures are collated and coordinated by establishing files to collect the information in desired categories

a Intelligence items pertaining to order of battle, state of training, operational planning, research and development activities, etc , are collected from plain-language traffic, from unit designations in the headings of messages and from operator chatter For example, the classified fact that an intercept station has certain facilities and personnel in various categories and is located at a given point can be derived from a collection of unclassified references to specific supplies and to military occupation classification numbers of the personnel The location might be given in the text or deduced from traffic routings Information leading to reconstruction of order of battle might be collected by noting unit locations, affiliations with other units, unit tables of organization (including names of key personnel), strengths of sub-units, specialties, activities, plans and equipment types and quantities These files of order of battle information are integrated with files on communication organization to give unit location as determined by direction finding, etc

b Security traffic analysts may also search for any evidence that could be used to assist in cryptanalysis of the traffic Operator chatter may reveal such information or a sequence of serial numbers may be indicative of an originator and thus make an encrypted signature predictable Recurrent stereotyped transmissions suggest effective lines of cryptanalytic attack and, presuming a knowledge of order of battle, the nature of the report may be predictable, further facilitating cryptanalysis

52Ø4 RECONSTRUCTION OF THE COMMUNICATION ORGANIZATION — Reconstruction of the communication organization is the basis for all traffic analysis It is necessary for the conduct of efficient intercept activities and it is the source of inference of intelligence regarding order of battle and military plans and operations Familiarity with the communication organization also makes it possible for the enemy to practice imitative deception and jamming Security analysts, therefore, examine traffic to determine to what extent the communication organization can be reconstructed and what intelligence can be extracted from external elements of transmission

a Purpose

(1) Effective intercept depends upon a knowledge of the communication organization (call signs, procedures, external traffic features, frequencies used, schedules of operation, etc) which makes possible the employment of equipment and personnel on circuits most productive of the type of traffic desired

(2) Direct intelligence in the form of order of battle can be obtained from a reconstruction of the communication system since the lines of communication are determined by military requirements and coincide with the chain of command This functional

characteristic of military communications must be considered constantly since it is the basis for many traffic analysis deductions

b Methods

(1) When the communication organization and operation are not disguised in any way, reconstruction is accomplished very simply by observation When call signs, frequencies, schedules, address groups, routing indicators, abbreviations, and other elements of a transmission are fixed, the significance of each element and its relationship to other elements is evident from consistent usage The reconstruction might progress by setting up a net diagram or a card file showing, for each communication center, data on each element as it becomes available The need for protective action in the form of disguised operation might be indicated if the organization as reconstructed were classified or if there were a compelling reason to avoid interception, as would be the case if security analysis could demonstrate that classified order of battle or other intelligence items could be assembled by foreign traffic analysis

(2) When the organization of the communication system is disguised by changing call signs, frequencies, times of transmission, etc , to make intercept and identification more confusing and difficult, reconstruction of the communication network is more complicated, proportionate with the care and thoroughness of the disguise Security traffic analysis has no single technique for testing the effectiveness of disguised operation since the multiplicity of disguise methods calls for a variety of traffic analysis methods

(a) Reconstruction of a well-disguised communication system may require the detailed analysis of a large volume of traffic collected over a long period of time Security traffic analysts' studies parallel assumed enemy efforts to reconstruct patterns and determine continuity of call signs, frequency allocation, serial number sequences, etc , by analysis of the elements of transmissions The analysis may take any form which will yield the information desired concerning the reconstruction of the organization, such as listing of stations transmitting on each frequency by transmission time, listing of serial number sequences, examination of services, plain-text and chatter

(b) Special identification techniques such as are involved in observation of hand-sending characteristics and in comparison of transmitter characteristics as shown on an oscilloscope and recorded on film are coordinated with the analyses Such studies will permit a fair evaluation of the success of disguise efforts

5205 PROCEDURE ANALYSIS — Procedure analysis is the examination of the elements of communication transmissions to determine malpractices in authorized transmission procedures in communication operations When detailed analysis of procedure is performed, discrepancy and violation key lists, which conform to standards established by Armed Forces Security Agency and are based on the applicable authoritative procedure publication, are employed to simplify and standardize the processing of traffic

5206 STATISTICAL STUDIES

a Tabulation of Elements of Transmission — Usually, the significant components of the transmissions to be studied are extracted from the monitored copy of the complete transmissions All data required for analysis and the compilation of files are recorded in convenient order and from this extracted data the traffic analyst makes the graphs, charts, and tabulations needed to study the traffic for the information desired in the particular mission Selection and tabulation of data can be performed mechanically by the use of IBM equipment when the volume of monitored traffic makes the use of such equipment feasible A card is punched to record the components of each message call, originator, addressee, system indicator, serial number, precedence, security classification, filing time, transmission time, group counts, etc The cards can then be sorted mechanically by any component as required for desired study

b Circuit Characteristics — Statistical studies are made to determine circuit characteristics such as directional flow of traffic, volume of traffic, precedence ratios, etc Continuing records of such studies made in repeated monitoring missions reveal changes in the network structure,

fluctuations in volume of traffic, increase or decrease of significant precedences, and other phenomena which reflect military activity and plans Statistical studies indicate the need for communication cover and provide the data necessary for effecting it

c Procedure Characteristics — Statistical records of detailed procedure analysis indicate trends in malpractices and show the need for amplification or revision of operating procedures Such studies may be of a general nature or confined to a single station, a group of stations, or a particular area

(1) Since tape relay traffic is transmitted in clearly delineated message units, the average number of malpractices for each message can be computed The nature of radiotelegraph or radiotelephone transmissions, however, makes such arbitrary demarcation unfeasible The malpractices for such traffic are computed on a "readable ' hourly basis to include call and reply, exchange of readability information, queries and repetitions of portions of the text, and other elements of procedure which are necessary in establishing contact and effecting the delivery of the message When radiotelegraph or radiotelephone circuits have been monitored, the circuit summary also includes notification of the number of hours the circuit was monitored and the indication of the actual transmission time monitored

(2) Progress charts showing the average number of malpractices for each message, or for each hour, may be kept for each station to compare successive discrepancy reports over a period of several months or years Such charts record the progress made by a station in improving its communication security or indicate what corrective action is needed

(3) Malpractices which are characteristic of a station and which could be used to identify the station, may be revealed by a chart showing the most frequently occurring malpractice for each station and what percentage of the total malpractices for all stations it represents

(4) Intelligence available to the enemy may be disclosed by a study of a station's malpractices on an hourly basis A characteristic of an operator may be reflected in such a study and could lead to deductions of the hours of work shifts and consequently the number of operators at the station Characteristic malpractices can be used to identify stations if call signs, operating schedules, or locations change

53ØØ - REPORTING TRANSMISSION SECURITY VIOLATIONS

53Ø1 GENERAL — Transmission security violations detected by transmission security monitoring and analysis activities are reported to responsible commands by such means as the situation warrants (see Section 44ØØ) If there is a possibility that the violation may produce immediate serious consequences, the report is made by the fastest means available Violations of less immediate importance may be reported through routine correspondence channels When required in tactical situations, provision should be made for rapid communications between monitoring units and liaison personnel to make possible the dissemination of vital information in time for protective measures to be taken

53Ø2 PROCEDURE DISCREPANCY REPORTS (COMMUNICATION IMPROVEMENT MEMORANDA) —When detailed analysis of transmission procedure is performed, procedure discrepancies are reported to the responsible command by Discrepancy Reports sent through routine correspondence channels

a Content — Procedure discrepancy reports may include identification of circuit monitored, period of monitoring, comparison of current discrepancy rate with results of previous monitoring, a description of each malpractice, number of times noted, and a citation of the authority violated Examples illustrating the most serious and most frequently recurring errors are selected from the monitor copy and included with the report The entire monitored copy, with discrepancies marked, may be sent with the report when the volume of traffic monitored is not large A circuit summary, giving a consolidated report of discrepancies for all monitored stations in a command, may be prepared for the responsible command

b Forwarding of Reports — Summary Procedure Discrepancy Reports (Communication Improvement Memoranda) are forwarded through routine channels to the responsible commands for action (with courtesy copies for individual stations monitored) Summary reports and special reports prepared by field monitoring and analysis organizations are sent to the Service Cryptologic Agencies as required

54ØØ - APPLICATIONS

54Ø1 COMMAND — The factors which transmission security analysis finds to be productive of intelligence indicate what aspects of communications need protection Commanders are advised of the degree of security prevailing in their communications, what intelligence the enemy may be expected to have obtained, and what means can be employed to minimize the intelligence obtainable through traffic analysis By demonstrating the extent of intelligence available to the enemy and the factors which make it available, traffic analysis enables commanders to strengthen the security of their communications by emphasis on circuit discipline or operator training, by reclassification of potentially informative material, or by the application of tactical communication cover and deception techniques devised by security traffic analysts to minimize the intelligence available through analysis

54Ø2 TECHNICAL — Service communication security agencies accumulate reports of analysis from their transmission security monitoring activities and the information provided by these studies is used as the basis for the constant revision and improvement of procedures in appropriate panels of the Joint and Combined Communications-Electronics Committees and as a basis for cover and deception plans to support military operations

INDEX

CONFIDENTIAL

AFSAG 1248

CONFIDENTIAL

ORIGINAL
(Reverse Blank)