

~~RESTRICTED~~*Free**AFSA**Attn. Mr. Friedman*~~RESTRICTED~~NORTH ATLANTIC MILITARY COMMITTEE
COMITE MILITAIRE DE L'ATLANTIQUE NORD

Standing Group

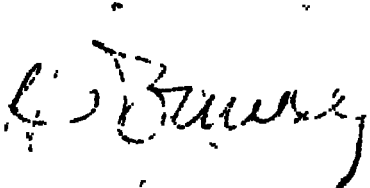
Groupe Permanent

SGM-201-50
20 July 1950MEMORANDUM FOR ALL MILITARY REPRESENTATIVES ACCREDITED
TO THE STANDING GROUP.SUBJECT: Regulations Governing the Handling and Use
of Cryptographic Material Provided for the
Use of the North Atlantic Treaty Organisation.

1. The annexed regulations governing the handling and use of cryptographic material provided for the use of the North Atlantic Treaty Organisation (which are supplementary to the basic security agreement contained in DC 2/1) have been approved by the Standing Group for transmission to the nations signatory to the North Atlantic Treaty.

2. The concurrence of member nations in these regulations is requested.

FOR THE STANDING GROUP:



C.H. DONNELLY
Colonel, USA
Secretary

~~RESTRICTED~~~~RESTRICTED~~

~~RESTRICTED~~

REGULATIONS GOVERNING THE HANDLING AND USE OF
CRYPTOGRAPHIC MATERIAL PROVIDED FOR THE USE OF
THE NORTH ATLANTIC TREATY ORGANISATION

1. SCOPE

a. Cryptography is a basic and widely employed method of protecting classified information transmitted by any means susceptible to interception. It is of paramount importance that the cryptographic material provided for the use of the North Atlantic Treaty Organisation be accorded a maximum degree of protection in all its phases of existence and use in order to insure that no information may be gained by unauthorised persons through compromise of such cryptographic material.

b. In order to safeguard such cryptographic material, it is imperative that the regulations establishing the protective measures to be afforded such material be standardized and rigidly observed. This document sets forth the basic protective measures considered essential to the proper safeguarding of such cryptographic material. The measures outlined herein are to be considered as minimum standards and may be elaborated upon as any of the signatories of the North Atlantic Treaty Organisation may deem necessary, desirable and practicable.

c. Two separate and distinct elements are embodied in any crypto system

(1) The basic or unchanging element which may consist of a principle, device, or machine.

(2) The specific element or variable key used in conjunction with the basic element.

Crypto systems provided for the use of the North Atlantic Treaty Organisation will be designed in such a manner that to a great degree their security depends upon safeguarding only the second of the two elements, but it is also essential to establish special safeguard for the protection of the basic element.

~~RESTRICTED~~

~~RESTRICTED~~

d. The measures which are outlined herein and which apply to all items of cryptographic material likely to be provided for the use of the North Atlantic Treaty Organisation, may be augmented from time to time with additional requirements for particular items of cryptographic material that may subsequently be provided.

2. AUTHORIZATION

a. No crypto system will be employed for North Atlantic Treaty Organisation purposes unless it has been approved by the Standing Group (Communications Electronics Coordinating Section) or higher authority.

b. No crypto system approved for the use of the North Atlantic Treaty Organisation shall be employed for any other purpose but that for which it has been provided without express permission of the Standing Group (Communications Electronics Coordinating Section). When a crypto system approved for the use of the North Atlantic Treaty Organisation is employed for other purposes than that for which it has been provided, such system will be safeguarded in accordance with the provisions of these regulations or such special regulations as may be issued by the Standing Group (Communications Electronic Coordinating Section).

c. Cryptographic principles, systems, or material provided for the use of the North Atlantic Treaty Organisation may not be reproduced or copied except with the prior approval of the Standing Group (Communications Electronics Coordinating Section).

d. Cryptographic material provided for the use of the North Atlantic Treaty Organisation will not be issued to, discussed with or shown to personnel or organisations of any nation which is not a signatory of the North Atlantic Treaty Organisation without the prior approval of the Standing Group (Communications Electronics Coordinating Section).

~~RESTRICTED~~

~~RESTRICTED~~

3. DEFINITIONS

a. APPROVED CIRCUITS. Electrical means of signal communication which have been approved by the Standing Group (Communications Electronics Coordinating Section) for the transmission in plain language of classified information of a specified security classification,

b. COMPROMISE. The capture, or recovery, by salvage, theft, photography, or cryptanalytic solution of cryptographic materials, plans, orders, and the like by unauthorized persons. (Physical compromise results when it must be concluded that, by reason of loss, theft, capture, recovery by salvage, or unauthorized viewing, cryptographic material has become available to unauthorized persons, Cryptographic compromise results when it must be concluded that, by reasons of cryptanalytic method applied to available communications, unauthorized persons may recover the plain text of messages sent in the crypto system affected or in a related system).

c. CLASS. Designations assigned to cryptographic holder grouped accordingly to similarity of requirements.

d. COMMUNICATION SECURITY. The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from a study of communications.

e. CRYPTOCENTER. An establishment maintenance for the encrypting and decrypting of messages.

f. CRYPTOGRAPHIC MATERIAL. All cryptographic equipment, instructions, and keying materials used in the encryption and decryption of classified communications.

g. CRYPTO SYSTEM. The associated items of cryptographic material which are used as a unit and which provide a single means of encryption and decryption of communications.

~~RESTRICTED~~

RESTRICTED

h. CRYPTO SECURITY. That component of communication security which results from the provision of technically sound crypto systems and their proper use.

i. CRYPTO SECURITY OFFICER. The officer appointed by the commander of a headquarters or other equivalent authority to represent the command or other equivalent agency in all matters relating to crypto security and the physical security of cryptographic material.

j. CUSTODIAN. The officer who is charged with the actual custody, handling, and safeguarding of registered documents issued and who is responsible to the Commanding Officer or other equivalent authority therefor.

k. EMERGENCY DESTRUCTION. The burning or destruction to such an extent as to render unrecognizable and unusable of cryptographic material when its capture is threatened, to prevent its being of value to unauthorized persons.

l. LITERAL TEXT. The verbatim plain-text transcription of encrypted text.

m. LONG TITLE. The descriptive name assigned to a document or device by the preparing agency.

n. PARAPHRASE. To change the phraseology of a message without changing its meaning.

o. PHYSICAL SECURITY. That component of communication security which results from all measures necessary to safeguard classified communication equipment and material from access thereto by unauthorized persons.

p. REGISTERED MATTER. Any classified matter taken on registered charge, and periodically accounted for.

q. REGISTER NUMBER. A number assigned to registered matter for accounting purposes.

RESTRICTED

~~RESTRICTED~~

f. ROUTINE DESTRUCTION. The burning or otherwise rendering useless of obsolete or surplus cryptographic material, as ordered by the office of issue.

g. SHORT TITLE. A short, identifying combination of letters and/or numbers assigned to a document or device for purposes of brevity and/or security.

t. TRANSMISSION SECURITY. That component of communication security which results from all measures designed to protect transmissions from interception and/or traffic analysis.

4. ALLOCATION, PREPARATION, DISTRIBUTION.

a. Allocation of cryptographic material will be determined by the Standing Group (Communications Electronics Coordinating Section) on the basis of requirements. To this end, holders of consumable material such as books of settings must notify the Standing Group (Communications Electronics Coordinating Section) as much in advance as possible when replacements are required.

b. The printing, reproduction and storage of cryptographic material by the agency responsible for its preparation will be performed in a manner which will safeguard the security of the information involved. Provision will be made for the proper safeguarding and destruction of notes, manuscripts, type, plates, stencils, negatives and waste in a manner commensurate with the classification of the material being prepared.

c. Each item of cryptographic material will show its classification, short title, and register number. Whenever possible, the long title, the office of origin, effective date, duration of effectiveness and instructions for accounting and ultimate disposal will be shown on the item. (When this is not possible this information will be published separately.)

~~RESTRICTED~~

RESTRICTED~~RESTRICTED~~

d. Distribution of cryptographic material to using organisation will be as direct as possible consistent with efficient and secure transmission of the material.

e. Cryptographic material will be securely packed for transmission, whenever practicable, in a double wrapping, with no indication of the contents or their classification on the outside wrapper. Packages containing cryptographic material will be covered by a receipt system during transmission.

f. Transmission of cryptographic material will be by couriers officially designated as such by competent authority, or by other approved means. When other approved means are used it is the responsibility of the distributing agency to assure itself that the means so utilized are wholly under the control of the nation(s) signatory to the North Atlantic Treaty concerned and the material is at no time subject to inspection or censorship.

(1) If possible, persons officially designated as couriers will not be assigned other duties during a courier trip and will deliver the cryptographic material before assuming any other duties. They will be instructed by the transmitting agency in the proper method of destroying the material in an emergency. The transmitting agency must be satisfied that the courier realises the necessity for the constant safeguarding of the material entrusted to him.

(2) Cryptographic machines (unless specifically excepted by the Standing Group (Communications Electronics Coordinating Section)) will be transmitted only in the custody of an officially designated courier

~~RESTRICTED~~**RESTRICTED**

RESTRICTED

irrespective of the type of transportation used and will also be handled in accordance with special instructions applicable to the particular equipment, except that when cryptographic machines are being shipped overseas they may be unaccompanied by a courier provided that:

(a) They are shipped in a naval vessel of one of the nations signatory to the North Atlantic Treaty, on charge to the Captain.

(b) They are shipped in a merchant vessel of one of the nations signatory to the North Atlantic Treaty, in charge of the Captain (who must have security clearance from the Shipping Government) and in locked stowage, and

(c) They are delivered in either event to the Captain by an officially designated courier and are collected from him by an officially designated courier at the port where they are landed.

g. The distribution of cryptographic material will be so arranged that each local distributing agency will have one or more reserve editions of each system available at all times. These reserve editions may be the next regular editions, received in advance, or may be spare editions permanently kept in reserve and placed in effect only upon proper notification.

h. When registered cryptographic material is transferred from one service or agency to another, the material will be incorporated in the accounting system of the receiving service or agency, will be handled and safeguarded in accordance with the security measures of the receiving service or agency and with these regulations. The classification of cryptographic material will not be changed without the approval of the originating authority.

RESTRICTED

~~RESTRICTED~~5. ACCOUNTING.a. By the Standing Group (Communications Electronics Coordinating Section).

(1) The Standing Group (Communications Electronics Coordinating Section) will maintain a central record of all registered cryptographic material allocated in accordance with paragraph 4 a, above.

(2) To this end North Atlantic Treaty nations will render to the Standing Group (Communications Electronics Coordinating Section) on 1 January and 1 July of each year certificates showing short titles and register numbers of:

(a) All registered cryptographic equipment still held and the command or agency by which it is held.

(b) All registered consumable cryptographic equipment (e.g. books of settings) destroyed during the past six months.

(c) All other registered cryptographic equipment destroyed (e.g. in an emergency) during the past six months.

b. By North Atlantic Treaty Organization Nations.

(1) In each command or other equivalent agency holding registered cryptographic material the commander or other equivalent authority will appoint an officer to be the custodian of cryptographic material. The custodian will be responsible for the proper safeguarding of, and accounting for all registered cryptographic material.

(2) Registered cryptographic material will not be considered as ordinary property but will be accounted for in a manner which will ensure that the material is being securely handled, stored and safeguarded at all times. The accounting system will provide for the maintenance of a complete record of each item of cryptographic material

~~RESTRICTED~~

~~RESTRICTED~~

by requiring the following:

(a) Notification of initial receipt of each item.

(b) Reports of inventory checks at least once every six months, and invariably on transfer to the charge of another Commanding Officer or other equivalent authority and/or custodian.

(c) Reports of transfer between individual custodians or organizations.

(d) Reports of destruction (routine and emergency)

Provided that these basic requirements are established, the accounting processes will be as prescribed by the individual services or other equivalent agencies.

6. STORAGE.

a. Registered cryptographic material will be stored in three combination safes or their equivalent.* Otherwise the material must be kept constantly under armed guard. The storage space containing registered cryptographic material will be kept locked when not under the supervision of authorized personnel.

b. As far as practicable, keying materials will not be stored in the same safe as the instructions or devices to which they apply. This restriction does not apply to a vault used exclusively for the storage of registered cryptographic materials.

c. Where, owing to its size a cypher machine cannot be stored in a safe when not in use, the basic or unchanging element (see paragraph 1 c (1) above) must be locked up or covered over and safeguarded against inspection by unauthorized persons.

d. Each command or other equivalent agency will maintain current records showing the short title, register numbers and dates of storage or withdrawal of all registered cryptographic material in storage or removed from storage by use or issue.

* As defined in the Basic Security Agreement for the North Atlantic Treaty Organization,

~~RESTRICTED~~

RESTRICTED

7. DUTIES AND RESPONSIBILITIES OF COMMANDERS OR OTHER EQUIVALENT AUTHORITY AND CUSTODIANS.

a. In each command or other equivalent agency holding cryptographic material, the commander or other equivalent authority will be responsible for all measures necessary to ensure crypto security and physical security of cryptographic material. The commander or other equivalent authority will, in accordance with the regulations of the several services or other equivalent agencies, appoint an officer to supervise cryptographic operations. This officer is called the "crypto security officer" and may also be appointed as custodian of cryptographic material.

b. All personnel engaged in cryptographic activities must be conscious of the need for, and cognizant of, the means of achieving maximum communication security. Continuous and effective security is possible only if each individual makes a determined effort to maintain the highest standards of procedure and operating techniques.

8. SECURITY OF INSTALLATION.

a. To provide maximum security the following will be observed in all installations:

(1) The crypto center will be established in a secure portion of the command or other equivalent agency, and not in an isolated location.

(2) If practicable the crypto center will be sound proof.

(3) If practicable fireproof safes and cabinets will be used.

(4) Windows will be non-transparent unless they are protected by shutters, blinds, louvres, or blackout curtains.

(5) At no time will unauthorized persons be permitted access to or an opportunity to view the cryptographic material in the crypto center.

RESTRICTED

~~RESTRICTED~~

(6) Normally the crypto center will be locked at all times.

b. The following will be observed at all shore installations and as far as possible on shipboard installations.

(1) The entrance will be constructed so that persons seeking admittance may be identified without permitting access to, or a view of, the interior of the crypto center.

(2) A notice that the crypto center is a restricted area will be displayed outside the door but the nature of the operations within will not be indicated.

(3) The windows of the crypto center will normally be barred and protected by wire mesh to prevent papers blowing away.

9. QUALIFICATIONS OF PERSONNEL.

a. Normally military personnel will be assigned to perform cryptographic duties. Before such personnel are so assigned their loyalty, reliability and trustworthiness will be confirmed by the commanding officer or other appropriate authority.

b. Civilian personnel may be selected to perform cryptographic duties. Before being so assigned they will be investigated in order to establish their trustworthiness, integrity, and loyalty.

c. No person will be assigned to cryptographic duties by any of the several services or other equivalent agencies if such individual is not a citizen or subject of the nation concerned, or a citizen or subject of a nation which is a signatory of the North Atlantic Treaty.

d. No person will be permitted to use cryptographic material unless he has been carefully instructed and thoroughly tested for efficiency in the procedure pertinent to the particular material.

~~RESTRICTED~~

~~RESTRICTED~~~~RESTRICTED~~

e. Should any person assigned to perform cryptographic duties be subsequently found to be unreliable, untrustworthy or disloyal, he should be immediately removed from such duties and the fact reported as grounds for suspecting compromise (see paragraph 10 below).

10. REPORTS OF COMPROMISE

a. The loss of suspected compromise of any cryptographic material, device or publication will be reported by the most expeditious means at hand to the Theater (Department, Force, Independent Command) Commander or other equivalent authority and the Service Head or other equivalent authority concerned who will inform the Standing Group (Communications Electronics Coordinating Section). The Theater (Department, Force, Independent Command) Commander or other equivalent authority may order discontinuance of the use of the compromise-suspected material, device or publication within his own command or other equivalent agency pending action by the Standing Group (Communications Electronics Coordinating Section).

b. When the circumstances of a compromise warrant such action proper authority will direct each commander or other equivalent authority to review all messages encrypted at his headquarters or other equivalent agency in the compromised system, take such action as he deems necessary and report to the next higher headquarters or other equivalent agency any compromise of information involving major operations, strategic intelligence or significant military plans.

c. In all cases of compromise a thorough investigation will be made into the circumstances. The report of this investigation will be forwarded to the Service Head or other equivalent authority concerned, who will inform the Standing Group (Communications Electronics Coordinating Section).

~~RESTRICTED~~~~RESTRICTED~~

~~RESTRICTED~~11. ROUTINE AND EMERGENCY DESTRUCTION.a. Routine Destruction.

- (1) Prior to destroying any cryptographic material, each item will be thoroughly checked to ascertain that only the material which should be destroyed is included.
- (2) Cryptographic documents will be destroyed by being burnt by authorized personnel or effectively pulped under authorized supervision when directed.

b. Precautionary Destruction.

Precautionary destruction to reduce the probability of capture or other physical compromise, may be undertaken by a local commander or other equivalent authority upon his own initiative or upon instructions received from higher authority. Such destruction will normally not include current or first reserve systems and will be accomplished as far as possible in advance of an anticipated emergency.

c. Emergency Destruction.

- (1) A plan will be adopted to ensure effective destruction of cryptographic material under emergency conditions. The specific steps taken will depend in each instance upon the conditions prevailing in the particular area and the likelihood of capture or loss.
 - (a) The plan will provide for sufficient officer and other personnel, including alternates, to carry out the expeditious destruction of cryptographic material at any time.
 - (b) The plan will assign responsibilities by watches or duties rather than by name.
 - (c) Frequent drills will be held to test the plan.

~~RESTRICTED~~

~~RESTRICTED~~

- (2) The following is the priority in which emergency destruction of cryptographic material should be carried out:-
- (a) Rotors, cipher key lists
 - (b) Cipher machines and associated material
 - (c) Other cryptographic material.
- (3) Cryptographic material which is of highest priority on the destruction list should be marked or stored in a clearly distinctive manner to ensure expeditious destruction.

12. TRANSMISSION SECURITY.

a. The regulations governing transmission of communication via electrical means are contained in other publications.

b. Classified messages will not be transmitted in plain language by electrical means except over circuits approved by the Standing Group (Communications Electronics Coordination Section) for the classification(s) concerned or in emergencies under procedures established by the individual services or other equivalent authorities.

~~RESTRICTED~~