

~~SECRET~~

USCIB: 13.5/42

8 March 1954

31

~~SECRET~~MEMORANDUM FOR THE MEMBERS OF USCIB:


Subject: Security of COMINT Transmitted by Electrical Means.

Reference: (a) USCIB 13.5/36 of 8 February 1954.
(b) USCIB 13.5/40 of 23 February 1954.

1. Reference (a) was circulated to the members of the Executive Committee on vote sheet. Reference (b) indicated a divergence of views with regard to reference (a).

2. At its Twelfth Meeting on 4 March 1954, USCIBEC considered the references and approved a compromise version of the "Proposed Security Requirements for Transmission of COMINT by Electrical Means" as set forth in the enclosure hereto. In order to clarify the changes agreed emendations to the enclosure with reference (a) are shown by employing dashes through proposed deletions and by underlining proposed additions.

3. In accordance with paragraph 11 of USCIB Directive Number 1 absence of objection to the enclosure herewith by 1700, Wednesday, 17 March 1954, will be considered to constitute Board approval.


RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure
a/s

USCIB: 13.5/42

~~SECRET~~

~~SECRET~~~~SECRET~~SECURITY REQUIREMENTS FOR TRANSMISSION
OF COMINT BY ELECTRICAL MEANS

1. Because of the great number of different operational situations, it is not possible to establish a firm set of detailed rules for handling COMINT information by electrical means which will be applicable in all circumstances or which will always guarantee security. It is possible, however, to state certain precepts and objectives which must be diligently pursued in order to maintain security and upon which detailed rules,* promulgated as circumstances require, must be based. The following paragraphs summarize the principles and describe briefly the method of achieving the objectives.

2. Cryptographic and communications plans must be considered in the early stages of planning for any new activity in the COMINT field in order to insure adequate cryptographic and transmission security. Experience shows that when plans for the establishment of a new unit have been finalized without any consideration having been given to communication requirements and their security aspects, resultant insecurities are often irreparable. Departments and agencies will are therefore urged to submit communication portions of plans for new COMINT activities to Director, NSA, for approval of the communication security aspects thereof before placing them in effect. During the preparation of these plans, the Director, NSA, will provide such assistance as may be requested.

3. It is desirable to avoid to the maximum practicable extent all external message characteristics which facilitate traffic analysis identification of traffic as a COMINT end product inasmuch as the transmission characteristics of traffic so identified is indicative of the effort expended or the success achieved by COMINT producers. Where possible, all evidences of direct communications between and direct cryptographic association of dissemination-consumer activities and collection-forwarding activities should be avoided. Where direct electrical communications are essential, appropriate steps should be taken to disguise the linkage. Cryptosystems identified exclusively with the collection-forwarding activities should not be held by dissemination-consumer activities. The Director, NSA, should be consulted in the selection of specific cryptosystems and the formulation of special cover procedures to be employed for direct electrical communications between collection-forwarding activities and dissemination-consumer activities.

4. COMINT communication operating methods and procedures will conform with those normally employed by the department or agency concerned.

* Detailed rules have been promulgated to elements under the operational or technical control of the Director, NSA, in accordance with paragraph 2e(4), NSCID No. 9 (Revised). Detailed rules to apply to all other COMINT communications will be promulgated by the Director, NSA, at an early date.

Enclosure with USCIB 13.5/42 dtd 8 Mar 1954.

~~SECRET~~

~~SECRET~~~~SECRET~~

Where military facilities are employed for transmission, approved military procedures will be employed. Wherever exceptions or modifications to operating procedures are required because of the nature of COMINT communications, they will be authorized by Director, NSA, ~~as-necessary~~ or by appeal to USCIB if necessary.

5. COMINT activities of an especially covert nature (e.g., those whose existence is considered sensitive because of geographical location or for political reasons) must not be issued cryptographic systems which are identified with other COMINT activities of a less covert nature, unless adequate provision is made for disguising traffic in such systems while in transmission. A special purpose system not identifiable by traffic analysis as an exclusively COMINT cryptosystem should be used and the external routing of messages should avoid overt association with other COMINT activities. Special systems and procedures will be provided by the Director, NSA, as necessary to meet requirements expressed by other agencies and departments.

6. Access to COMINT information in encrypted form can be effectively controlled only if COMINT information is transmitted in cryptosystems specifically authorized for such use. This authorization will be provided by the Director, NSA, upon request from agencies and departments.

7. Keying material used for COMINT information will be issued only to those persons and activities authorized access to COMINT. Keying material used for COMINT will not be used for non-COMINT information except in ~~emergency~~ unusual conditions ~~or as approved by the Director, NSA.~~ It should be noted that logistical and administrative messages pertaining directly to the support of a COMINT activity ~~must~~ may be considered COMINT information.

8. Only those operating instructions, keying materials, and other crypto-aids prepared or approved by the Director, NSA, are authorized for use in encrypting COMINT information.

9. Programs and facilities for training personnel in cryptographic operations, maintenance, and other COMSEC specialties, adequate to insure maximum possible proficiency must be maintained and kept under continuing review by agencies and departments. Procedures must be established to insure that only those individuals with proper training are permitted to operate cryptosystems or maintain cryptosecurity equipment. Technical guidance and support for COMSEC training will be provided by the Director, NSA.

10. Training editions of cryptosystems of a type used exclusively for COMINT operations will be made available only to authorized training activities; training in such systems must be restricted to personnel to be assigned to COMINT activities.

~~SECRET~~

~~SECRET~~~~SECRET~~

11. One of the principal sources of compromise in COMINT communications is the inadvertent transmission of plain language or the transmission of improperly encrypted messages in on-line cryptographic operation. It is essential that operators be thoroughly trained in the operating procedures and use of the equipment and that full use be made of equipment and devices designed to guard against the occurrences of insecure transmissions.

12. Cryptographic systems for use in COMINT collaboration with foreign countries are to be made effective only by the Director, NSA.

13. Electronic and electromechanical equipment must not be used in such a manner as to jeopardize COMINT information due to intelligence-bearing radiations. Policies governing this aspect of the use of security equipment for transmitting COMINT will be established by the Director, NSA.

14. COMINT information shall not be transmitted in plain language by electrical means except in accordance with USCIB-approved policies.

15. Wherever feasible, the encryption and decryption of COMINT information should be carried out in an area devoted exclusively to these purposes.

16. All personnel engaged in the handling of COMINT information shall be subject to the security investigations, clearances, and indoctrination as are prescribed in USCIB Directive No. 5.

~~SECRET~~