

USCIB: 13.5/85

21 October 1954

~~TOP SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of COMINT Due to Ineffective Communications Security.

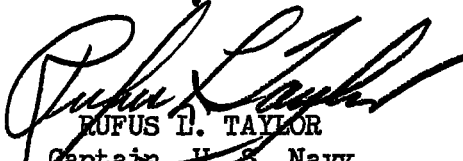
References: (a) USCIB 13.5/68 of 24 May 1954.
(b) USCIB 13.5/81 of 15 June 1954.

1. The enclosures herewith are circulated for information. LSIB/119/54 was circulated under cover of reference (a).

2. Particular attention is invited to paragraph 5 of enclosure 1.

3. With regard to paragraph 3 of enclosure 1, the Executive Secretary has prepared a memorandum for the Secretary, LSIB setting forth in general terms action taken and contemplated by USCIB in this matter. It is included herewith as enclosure 2.

4. If there is no objection by any member prior to the close of business, Friday, 29 October 1954, enclosure 2 will be forwarded to the Secretary, LSIB.


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

Enclosures

1. LSIB/338/54 dtd 7 Oct 1954.
2. Memo for Secy., LSIB.

USCIB: 13.5/85

GOVERNMENT COMMUNICATIONS HEADQUARTERS,
OAKLEY, CHELTENHAM, GLOS.

LSIB/338/54

7th October, 1954.

~~SECRET~~

Executive Secretary,
U.S.C.I.B.

COMPROMISE OF SIGINT CODEWORDS AND/OR MATERIAL.

Reference my LSIB/119/54[†] of 6th May 1954, L.S.I.B. has again considered the compromise of Sigint information arising from the misuse of Sigint telecommunications.

2. In accordance with the provisions of the UKUSA agreement the Directors of N.S.A. and G.C.H.Q. have exchanged reports on the compromises committed by their respective nationals.

3. L.S.I.B. is deeply concerned at the continued breaches of security by both parties, and would be grateful to know of any action your Board may have in mind to reduce this danger to our common effort. L.S.I.B. will inform you of any further action it intends to take to the same end.

4. L.S.I.B. suggests that an exchange of views on this question would be valuable so that each party may be aware of any special precautions which have been instituted by the other to improve security.

5. At the same time, L.S.I.B. would like to suggest that the reports exchanged between the two Agencies should contain details of the cause of the compromise, whether mechanical or human. It would then be possible to effect a more detailed analysis of the reasons for this threat to our common interests and subsequently to introduce more effective remedial measures.

PL 86-36/50 USC 3605

/s/

[Redacted Signature]

Secretary,

London Signal Intelligence Board.

[†]Memorandum forwarded to Executive Secretary U.S.C.I.B.
as approved by the Senior Board at LSIB(54)7th Meeting.

Enclosure 1 with USCIB 13.5/85 dtd 21 Oct 1954.

~~TOP SECRET~~

CIB #000273

~~TOP SECRET~~MEMORANDUM FOR THE SECRETARY, LSIB:

Subject: Compromises of COMINT Codewords and/or Materials.

Reference: LSIB/338/54 of 7 October 1954.

1. USCIB has for some time been deeply concerned by the matter you mention in the reference and regards this source of leakage a most dangerous security weakness capable of rendering all other security efforts impotent.

2. Accordingly, in August of 1953 USCIB directed corrective action which, as an initial step, resulted in USCIB Directive Number 9, at the same time USCIB commented as follows:

"Experience has demonstrated that even if cryptographic systems and procedures are sound, good communications security can be achieved only through elimination of poor practices and personnel failures."

3. Subsequently the Director, NSA was asked by USCIB to submit a status report on action taken to improve communications security in the COMINT elements under his operational and technical control together with any recommendations he might deem appropriate.

4. In responding to this request the Director, NSA reviewed the various actions which have been taken to eliminate plain language transmission in on-line operations, the status of crypto systems employed for COMINT transmission, communications security surveillance and compromise reporting procedures, and then listed certain additional action as set forth in enclosure 1 hereto.

5. In his general comment the Director, NSA included the following remarks:

"Of the total compromises to date of COMINT information due to communications insecurities, a small number have been traceable to faulty equipment. A somewhat larger number have resulted from cryptographic violations, - either failure of the cryptographers to comply with the operating instructions for the cryptosystem concerned, or failure to perform properly and completely the check-decryption process. Errors in this category are ordinarily due to partial ignorance of the rules or insufficient training and experience in

Enclosure 2 with USCIB 13.5/85 dtd 21 Oct 1954.

~~TOP SECRET~~

~~TOP SECRET~~

GIB #000273

~~TOP SECRET~~

Subject: Compromises of COMINT Codewords and/or Materials.

their application, and less frequently to inattention or carelessness. Additional training and experience, therefore, can be expected to result in a degree of technical competence that could virtually eliminate this type of error.

"Technical competence in the operation of crypto-aids, however, is not enough. It is an alarming fact that more than half of all compromises of COMINT information continue to involve transmission in the clear on interceptible wire or radio circuits; and it is an additional cause for concern to note the high percentages of these clear text transmissions that are due directly to inattention or carelessness on the part of the operators. It will be noted that, in the corrective action outlined in the inclosed report, attention has in the past been focused on equipments and procedures, and the main effort has been expended in improving both. It is the Director's opinion that, in improving the tools, and issuing the instructions, too little attention perhaps has been given to the fallible human beings who must use the tools and follow the instructions. For this reason, preventive and corrective action in the future should place increased and continued emphasis on specific guides and criteria for the training and indoctrination of personnel, and on the basic responsibility of command to develop in subordinates a deep sense of personal responsibility for the maintenance of communications security."

6. USCIB approved the above mentioned report of the Director, NSA and directed that all member departments and agencies cooperate in carrying out the program outlined therein (see enclosures herewith).

7. USCIB is hopeful that this campaign will result in the desired improvement.

8. With regard to paragraph 5 of the reference it is suggested that the Directors, GCHQ and NSA collaborate as necessary to exchange the information desired.

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

Enclosures

1. Part III of NSA Serial
 000407, 3 Sep 1954.
2. Encl. with USCIB 13.5/42.

- 2 -

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~PART IIIAdditional Action Contemplated

1. Issue to the Service Cryptologic Agencies for further issue to the elements under the operational or technical control of the Director, NSA, of detailed check-off lists covering general, cryptographic and transmission security and the physical security of cryptographic material, with separate detailed check items for each cryptosystem authorized for use by the field stations. It is intended that these check-off lists be used on receipt by the Commanding Officer or Officer in Charge of each COMINT activity in the conduct of an immediate inspection of his activity, and that the completed check-off list be returned to NSA and a copy furnished the Headquarters of the Service Cryptologic Agency concerned. A statement of any corrective action indicated and contemplated as a result of this inspection should accompany the completed check-off list. These inspections should be repeated at least every six months. It is intended also that these inspections by local command authorities are to be conducted in addition to, and not in lieu of, any scheduled or periodic inspections now conducted by higher authorities within the Service concerned.

2. An additional plan, utilizing the same check-off list as above, is also under consideration. The extent to which this plan would be developed would be dependent on the availability in NSA of qualified personnel who could be spared for the purpose. Under this plan, the Service Field Activities would be notified of the availability of Training Visit Teams provided by NSA. An officer fully qualified in all phases of COMSEC as applied to COMINT would, on request, conduct an informal instructional visit to the field station. In order to preserve the unofficial nature of the visit, it would be emphasized that its purpose primarily was instruction, not inspection. The check-off list would be covered in detail, the reasons behind the various rules would be discussed and explained, and specific recommendations for improvement of COMSEC at the station would be made to the Commanding Officer or Officer in Charge. The check-off list, after explanation and discussion, would be left at the station for future guidance and reference. Requests for training visits would be addressed to the Director, NSA, via the Head of the Service Cryptologic Agency concerned.

3. Specific COMSEC training criteria for the guidance of Commanding Officers and Officers in Charge of COMINT activities will be established and forwarded to the Service Cryptologic Agencies for implementation in all activities under their administrative control.

Enclosure 1 with CIB #000273.

~~TOP SECRET~~

~~TOP SECRET~~

4. The approved minimum standards as outlined in USCIB 13.5/42 dated 8 March 1954 will be summarized in an NSA Circular for the information and guidance of COMINT field activities. In addition to the listing of the standards themselves, specific recommendations and suggestions will be included to facilitate conformance with these standards.

~~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 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.

Enclosure 2 with CIB #000273.

~~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, 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 unusual conditions. It should be noted that logistical and administrative messages pertaining directly to the support of a COMINT activity 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~~

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.