

USCIB: 13/358

~~APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL~~

10 August 1953

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB/USCIBEC:

Subject: Compromise of COMINT Information.

Reference: (a) USCIB 13/334 of 8 May 1953.
(b) USCIB 13/338 of 28 May 1953.
(c) USCIB 13/339 of 29 May 1953.
(d) USCIB 13/340 of 3 June 1953.
(e) USCIB 13/355 of 29 July 1953.

1. Reference (b) is a summary of compromises of COMINT information by U. S. activities from November 1952 to March 1953. Reference (a) is a report of a compromise that should have been included in reference (b) but for some reason or other was not. References (c) and (d) are reports of U. S. compromises subsequent to the summary contained in reference (b). Reference (e) is a summary of British compromises that have occurred "in the past few months". The enclosure is a report of an additional U. S. compromise submitted in accordance with the enclosure to USCIB 13/308, together with certain views of the Director, National Security Agency, with regard to change of codewords.

EO 3.3(h)(2)

PL 86-36/50 USC 3605

2. An examination of the references and the enclosure reveal that out of a total of 25 reported U. S. and British compromises 22 were due to ineffective communications security, 1 was due to loss of accountability of a document, 1 was due to an error in marking documents for mailing, and the remaining one was due to careless telephone conversation. Breaking this down into U. S. and British



3. In the enclosure the Director, National Security Agency, questions the advantage to be gained in changing codewords. The Executive Secretary, USCIB, concurs in the view expressed. Changing codewords would appear to serve only the purpose of denying to foreign intelligence efforts the knowledge as to under what guise should our COMINT information be sought. A glance at the nature of

~~APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL~~

USCIB: 13/358

- 1 -

~~TOP SECRET~~

~~TOP SECRET~~
SECURITY INFORMATION

USCIB: 13/358

EO 3.3(h) (2)
PL 86-36/50 USC 3605~~TOP SECRET - SECURITY INFORMATION~~Subject: Compromise of COMINT Information.

our compromises reveals that foreign efforts need no such assistance. It seems clear that far too much emphasis has been placed on the magic of codewords and not enough on a practical overhaul of communications procedures and discipline.

4. Experience in the Armed Forces has demonstrated that even if crypto-systems and procedures are sound, good communications security can be achieved only through elimination of poor practices and personnel failures. This can be accomplished by a continuing program of education and training directed through commanding officers and by an unrelenting application of disciplinary action which carefully scrutinizes and impartially criticizes the actions of commanding officers as well as of those of the individuals directly performing communications duties. The Executive Secretary recommends that USCIB adopt such a program forthwith and do all in its power to persuade LSIB to do likewise.

5. It should be noted that the 11 U. S. compromises attributable to communications failures all occurred in so-called technical

Whatever the causes, it can happen to the consumers as well as to the processors. Paragraph 2e(4) of NSCID #9 (revised) places on the Director, NSA, responsibilities for prescribing and enforcing requisite security regulations for those elements under his operational or technical control. It would appear to be appropriate for USCIB to suggest that the Director, NSA, include in any action he may contemplate the steps outlined below insofar as elements under his technical or operational control are concerned, and, in order to minimize the likelihood of still further compromises, to direct that he extend his inspection and advice in communications matters pertinent to the security of COMINT to all elements under the cognizance of USCIB.

6. Accordingly, it is recommended that the Director, NSA, be directed by USCIB to:

a. Immediately conduct an investigation by inspection if necessary of the crypto-systems, procedures, practices, and training programs used by all member departments and agencies of USCIB for accomplishing the transmission of COMINT by electrical means.

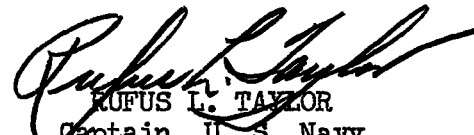
USCIB: 13/358

- 2 -

~~TOP SECRET~~

~~TOP SECRET - SECURITY INFORMATION~~Subject: Compromise of COMINT Information.

- b. Report to each member thus investigated the deficiencies noted together with recommendations for their correction, including a request for a report from the member concerned to the Director, NSA, of the action taken to correct the deficiencies noted.
- c. Report as soon as practicable to USCIB any uncorrected deficiencies together with the reasons therefor.
- d. Repeat the above process on a semiannual basis.
- e. In each case of compromise involving ineffective communications security, obtain a report which will include:
- (1) A formal report of investigation by the officer in charge of the activity concerned (to include a brief description of his training program for security).
 - (2) Statements from the individuals involved.
 - (3) A statement of what corrective and disciplinary action, if any, has been taken or is contemplated.
- f. If dissatisfied with the results of paragraph 6e above, report the circumstances to USCIB together with appropriate recommendations.
- g. Collaborate with the Director, GCHQ, and the Director, CB, in an effort to standardize the equipment, procedures, practice, training, and the level of discipline required to maintain effective communications security insofar as it relates to COMINT information and report to USCIB if not satisfied with the actions of the Director, GCHQ, or of the Director, CB.
7. This item will be placed on the agenda for the next regular meeting of USCIBEC.



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

Enclosure

DIRNSA Ser 000419-S of 4 Aug 53.

USCIB: 13/358

- 3 -

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.

C
O
P
Y

Serial: 000419-S

4 AUG 1953

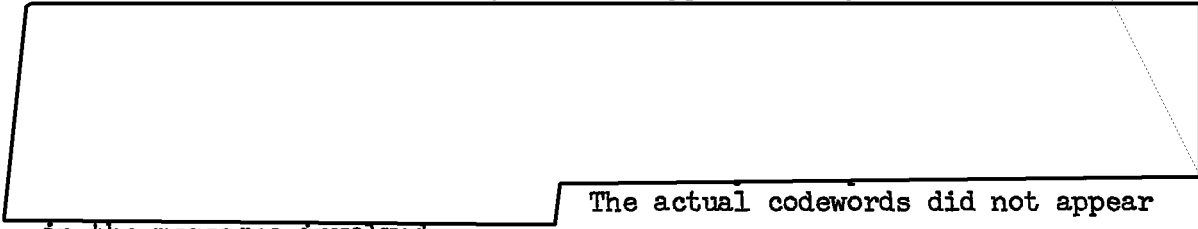
~~TOP SECRET CANOE - SECURITY INFORMATION~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

MEMORANDUM FOR THE EXECUTIVE SECRETARY, USCIB

SUBJECT: Possible Compromise of COMINT Information

1. I regret to inform you of a cryptosecurity violation which



The actual codewords did not appear in the messages involved.

2. Although no reaction has been observed to date in foreign communications, these messages, nevertheless, must be considered as having been subjected to compromise since their transmission was not immune to interception. Counting the possible compromises reported in the GCHQ letter of 16 July and previous ones reported by me, the total possible compromises to date of codeword material or the codewords CANOE and CHUTE since the last change is 24. It is recognized that one, or only a few compromises, may not be serious, but the cumulative effect of several, or many, may well be. Nevertheless, I see no real security advantage to be gained in changing codewords prior to normal expiration date as the Director, GCHQ, recommended. However, I will not oppose a recommendation for change if it is presented to USCIB by LSIB.

3. The Director, GCHQ, has been requested to inform appropriate British officials. The foregoing is submitted in accordance with the Inclosure to USCIB: 13/308.

(Signed)
RALPH J. CANINE
Lieutenant General, US Army
Director

Enclosure with USCIB 13/358 dated 10 Aug 1953.