STANDARD FORM NO. 64

~~TOP SECRET~~ FREE ID: 2598047 SECURITY INFORMATION

TS 52 117-CR
Copy #3

Office Memorandum • UNITED STATES GOVERNMENT

TO : Deputy USCIB Coordinator DATE:

FROM : Chief of Staff

SUBJECT: Separate Codeword for Cryptanalytic Methods

1. The Director has reviewed the procedures proposed for a separate codeword for analytic methods as contained in a memorandum to you, dated 5 May 1952, from the Chairman, USCIB Security Committee (SECCOM). As a result of this review, it has been determined that the AFSA position on this matter remains substantially the same as that contained in your memorandum on this subject, dated 15 January 1952, to the Chairman, SECCOM.

2. The attached draft memorandum (Inclosure) for the Chairman, SECCOM, contains a firm AFSA policy position on this matter and maintains that separate codewords for cryptanalytic methods and COMINT end products should be provided. It is therefore recommended that the Inclosure be forwarded to the Chairman, SECCOM, for consideration.

ALFRED R. MARCY
Colonel, Signal Corps
Chief of Staff

Inclosure - 1
Codeword for Analytic Methods

cc: Off/Operations
Off/COMSEC
Consultant

~~TOP SECRET~~

~~TOP SECRET~~ [illegible]

MEMORANDUM FOR THE CHAIRMAN, USCIB SECURITY COMMITTEE

SUBJECT: Codeword for Analytic Methods

1. In accordance with the recommendation contained in your memorandum of 5 May 1952, the Director, AFSA, has been afforded the opportunity to review the procedures which have been proposed for establishing a separate codeword for cryptanalytic methods. As a result of this review, a firm AFSA policy position has been established which is presented in the following paragraphs.

2. The AFSA position on this matter remains substantially the same as that forwarded for your consideration in my memorandum of 15 January 1952. In addition, the following comments resulted from DIRAFSA's study of your memorandum of 5 May 1952:

a. By the BRUSA Agreement, the basic definition of COMINT and of its two categories, special intelligence and traffic intelligence, relates to the end product. Historically, this has been the case since the very first codeword was used. The intention was to require the intelligence so classified to be handled in such a way as to protect the source. In addition, the BRUSA Agreement stipulates that TOP SECRET codeword protection shall be accorded to techniques related to the end product in order to minimize the possible inference derivable about COMINT successes. However, the two fields of cryptanalytic method and COMINT results are, in general, quite separate, both as to material included and personnel involved. Therefore, the application of separate codewords to them is quite feasible. In the limited area of overlap, the convention could be that the product codeword alone would be used since its protection implies the protection of the source and thereby the method.

b. The responsibility of the Director, AFSA, to maintain adequate security procedures within the COMSEC field is being fully discharged. The desire to establish a separate methods codeword is meant to reinforce even further security procedures within a particular segment of the COMSEC field. In the light of this, the implication that a danger to the security of COMINT would arise if COMSEC methods were to be raised to the same category appears to be rather fallacious. Since

~~TOP SECRET~~

there is a much stricter limitation of COMSEC methods to the "need to know" principle, the danger to the security of COMINT by the establishment of a separate methods codeword is not evident. This is further substantiated by the fact that there are virtually no consumers of this material outside of AFSA and, consequently, compromise is unlikely since there is little or no dissemination in any form.

3. At the recent US/UK Communication Security Conference, this subject was discussed with members of the London Cypher Policy Board. The opinions that were expressed on this matter were as follows:

a. The UK representatives stated that, in their opinion, a single codeword for documents containing methods and techniques, as distinguished from the codeword for documents containing only the end products of COMINT operations, would result in greater protection for the COMINT end products. This opinion was based on the fact that a fair number of people who would require indoctrination for the methods codeword would no longer require indoctrination for the end product codeword.

b. The US representatives felt that the provision of a separate codeword would result in increased security for cryptanalytic methods and techniques. Material of considerable cryptanalytic importance, currently unprotected by codeword, could, under the proposal, be distributed with a greater measure of security than is now possible.

c. Both the US and UK representatives agreed that the proposed division would simplify the problem of indoctrination. In one case, it would be unnecessary to divulge the content or nature of the COMINT end product to persons concerned only with methods and techniques. The corollary of this would follow with respect to the indoctrination of those concerned only with the possession and evaluation of the COMINT end product.

d. It was also felt that, once having adopted a codeword for methods documents, there would seldom be necessity for changing the word on account of its actual or suspected compromise; further, it was felt that the codeword itself need not be classified as is the codeword for the end product.

4. Therefore, the USCIB Coordinator requests that you re-examine the procedures for establishing a codeword for analytic methods, as proposed in your memorandum of 5 May 1952, in the light of the AFSA policy position noted above, and the agreement reached on this matter between the US and UK representatives at the recent Communication Security Conference.