

~~TOP-SECRET SECURITY INFORMATION~~~~TOP SECRET SECURITY INFORMATION~~

3 September 1952

*Approved copy
9/9/52*

MEMORANDUM FOR THE MEMBERS, USCIB SECURITY COMMITTEE

SUBJECT: Codeword for Analytic Methods

There is attached a draft memorandum on this subject for the Coordinator which contains the conclusions and recommendations which the Committee reached at its meeting on 27 August 1952.

It is requested that you advise the undersigned of any changes or corrections which you desire to have made in this draft memorandum by telephone or in writing prior to the close of business on Monday, 8 September 1952.

Robert F. Packard

ROBERT F. PACKARD
Chairman, USCIB Security Committee

Encl

Draft Memorandum for the
Coordinator

~~TOP-SECRET SECURITY INFORMATION~~

~~DRAFT~~~~TOP SECRET SECURITY INFORMATION~~
~~TOP SECRET SECURITY INFORMATION~~

3 September 1952

MEMORANDUM FOR THE USCIB COORDINATOR

SUBJECT: Codeword for Analytic Methods

1. Reference is made to the memorandum on this subject from the Coordinator to SECOM dated 15 January 1952 and 16 July 1952 and to SECOM's interim report to the Coordinator of 5 May 1952.

2. The Security Committee has reconsidered this problem in the light of the recent memorandum from the Coordinator and has reached the conclusions which are outlined below. These conclusions differ in part from those contained in the Committee's interim report to the Coordinator.

3. The Committee has concluded that, within the COMINT field, cryptanalytic methods and techniques can be protected adequately, if handled in accordance with the existing provisions for the protection of Special Intelligence and Traffic Intelligence, as appropriate. It is felt that the establishment of a separate category or sub-category of COMINT and the use of a separate codeword for cryptanalytic methods and techniques is not necessary, and would not necessarily afford additional security protection. As a corollary, it is felt that this is equally true as it would apply to the protection of COMINT products. These views are based on the following factors.

~~TOP SECRET SECURITY INFORMATION~~

~~TOP SECRET SECURITY INFORMATION~~
~~TOP SECRET SECURITY INFORMATION~~

a. Security protection of information concerning cryptanalytic methods and techniques must rest primarily on proper control over the distribution of this information, i.e.: strict application of the "need-to-know". This principle applies equally and is as applicable in the field of methods and techniques as in the field of COMINT production.

b. Information concerning methods and techniques is not entirely separable from information contained in products. This is particularly true as regards Traffic Intelligence. It would not be possible to create a separate package for all information dealing exclusively with methods and techniques. The resulting overlap would be confusing and could not be handled properly by the use of either a methods codeword or a products codeword for information in this area of overlap.

c. There is no need for producing personnel in AFSA or for consumer agencies to receive information dealing with methods and techniques except in those specific instances where that information is pre-requisite to proper intelligence use of COMINT products. Nor is it necessary for cryptanalysts to receive COMINT products save in those specific instances where the

~~TOP SECRET SECURITY INFORMATION~~

~~TOP SECRET SECURITY INFORMATION~~

information contained in these products is prerequisite to their analytic tasks. These distinctions can be enforced adequately within the framework of existing codewords, as indeed they appear to be at present.

4. Indoctrination for Special Intelligence or Traffic Intelligence does not require that, on the one hand, the content of COMINT products be divulged to persons concerned only with methods and techniques or that, on the other, methods or techniques be divulged to persons concerned only with the production of end-products. Indoctrination required only that all persons be instructed as to the nature of COMINT activities, the security practices governing them and the specific tasks to which they are assigned.

4. The Committee has concluded that, in the communications security (COMSEC) field, optimum security protection for cryptanalytic methods and techniques would be realized by application of the existing security practices for Special Intelligence or Traffic Intelligence, as appropriate, wherever this information (a) involves references to foreign communications or (b) is similar to those used, or likely to be used, in the COMINT field. As a corollary, it is felt that COMINT products would be adequately protected within the COMSEC field under such an arrangement. These views are based on the following factors:

~~TOP SECRET SECURITY INFORMATION~~

a. The Coordinator's memorandum of 16 July indicates that COMINT practices are not derogated by the present means of handling cryptanalytic methods and techniques in the COMSEC field and that the security protection of COMINT products would not be threatened by application of COMINT practices to the handling of cryptanalytic methods and techniques in the COMSEC field.

b. No unique security practice or separate use of a codeword for the protection of methods and techniques, similar to that applied in the COMINT field, has been evolved or suggested for the COMSEC field.

c. Use of the present COMINT codewords in the COMSEC field would be consistent with those provisions of Appendix B of the BRUSA Agreement which state that technical matter appertaining to the production of Special Intelligence or Traffic Intelligence shall be designated by the appropriate codewords and that communications which reveal actual success, progress or process in the production of Special Intelligence or Traffic Intelligence shall bear the appropriate codewords.

d. Application of the present COMINT codewords to methods and techniques in the COMSEC field would be consonant with British practice save in those instances

~~TOP SECRET SECURITY INFORMATION~~ ~~TOP SECRET SECURITY INFORMATION~~

where the British may apply COMINT codewords to COMSEC information which does not involve foreign communications or methods similar to, or expected to be applicable to, analysis in the COMINT field.

5. If, in the future, circumstances are changed so as to require the establishment of a separate codeword for analytic methods, there is provision in the proposed revision of Appendix B whereby this could be done through the establishment of an additional category or sub-category of COMINT.

6. The Security Committee recommends, therefore, that:

a. No separate codeword be established for analytic methods at this time.

b. That the present security practices for handling Special Intelligence and Traffic Intelligence and the present codewords, as appropriate, be applied within the COMSEC field to that information about cryptanalytic methods and techniques which involves either (1) foreign communications or (2) methods similar to, or expected to be applicable to, methods and techniques used in the COMINT field.

ROBERT F. PACKARD
Chairman, USCIB Security Committee

~~TOP SECRET SECURITY INFORMATION~~