

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

26 May 1952

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

MEMORANDUM FOR DEAR ADMIRAL WELCH

SUBJECT: Separate Code Word for Classified Documents containing details of Cryptanalytic Methods and Techniques

1. The memorandum dated 5 May 1952 for the Deputy USCIB Coordinator from the USCIB Security Committee on the foregoing subject was discussed informally on 23 May with representatives of the [redacted]

[redacted] and with representatives of AFSA (Mr. E. H. Shaw and Mr. C. G. Curry). It was the sense of the group that the provision of a separate code word for the indicated type of documents would be of real advantage.

2. The UK representatives stated that in their opinion a code word for documents containing methods and techniques, as distinguished from the code word for documents containing only the end products of COMINT operations, in other words, decrypts, would result, in the UK, in greater protection for the COMINT end products, to the extent that a fair number of people who would require indoctrination for the methods code word would no longer require indoctrination for the end product code word.

3. It was felt by the US representatives that the provision of a separate code word would result in increased security for the methods and techniques, in view of the fact that material of considerable cryptanalytic import now unprotected by code word could, under the proposal, receive the highly limited distribution which the material deserves.

4. It was felt by both sides that the problem of indoctrination would become much simpler and more logical given the proposed division, in that it would be unnecessary to make any mention of the content or nature of the COMINT end product to persons concerned only with methods and techniques, and in that it would be unnecessary to divulge to those persons concerned only with possession and evaluation of the COMINT end product the highly classified methods and techniques used in the derivation of that end product.

5. It was also felt that once having adopted a code word 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 code word itself need not be classified as is the code word for the end product.

6. It is therefore recommended that the USCIB Coordinator adhere to the position that separate code words for cryptanalytic methods and COMINT end products should be provided.

WILLIAM F. FRIEDMAN
 Consultant

~~TOP SECRET~~