~~SECRET~~

9 June 1954

To: Mr. Friedman

From: Mr. Callimahos, TWG

Subject: Security Classification of Training Document NSA-72-1678

Reference: T/S Telegram dated 9 March 1954 from Director, GCHQ, to Brig. Tiltman, SLO

1. The U.K. objection to the inclusion at the CONFIDENTIAL level of the information in para 6.54 of the PROD publication, "Current Cryptanalytic Techniques", comes somewhat as a surprise. Frankly, I can see no reason why any of the subparagraphs 6.54a through 6.54f merit a classification any higher than CONFIDENTIAL. It is true that all of these subparagraphs have at one time or another covered operational systems; but it is also true that many portions of other cryptologic training texts, CONFIDENTIAL and even unclassified, have or have had operational practicability.

2. There is no question in my mind that, in subparagraph 6.54, all the items but b and f are straightforward cryptographic aspects. Item f is but a slight departure from the obvious; but item b has been used time and again when other faster means of generation have not been employed. The entire substance of paragraph 6.54 deals with the cryptography of sources of additive, without one word on cryptanalysis; there is not the slightest indication that these sources of additive can be exploited. I realize that the objection to 6.54 must be item b, because of its applicability to certain sensitive problems--are we then to put psychological random's head in the sand and deny its existence?

3. As for the general statement in the referenced telegram that "this is a particularly striking example of the tendency to include in this handbook information that ought to be graded TOP SECRET Codeword", I have read carefully through the entire three volumes of the training document in question and I cannot find anything which to my mind would warrant exclusion from the standpoint of a CONFIDENTIAL document. At any rate, I think it pertinent to note that the PROD division which originally prepared and issued this document is going to replace it soon with another which they hope will be without objection.

4. In paragraph 4 of the referenced telegram it is stated that the syllabus of the Military Cryptanalytics series shows that "Parts I through IV are correctly graded CONFIDENTIAL since they are concerned

~~SECRET~~

with techniques that have repeatedly been described in published literature." Is it the U.K. view, then, that items appearing in the public domain are automatically classified CONFIDENTIAL? Actually, it is projected that Parts I through IV will contain much material that has not appeared in the public domain, but this material is not expected to transcend information to which we normally ascribe a CONFIDENTIAL classification.

5. As for the objection that the syllabuses of Parts V and VI "seem to us to cover secret processes that are currently in use at GCHQ for production of Category III COMINT and are therefore technical material within the meaning of Note 1B to Appendix B requiring the grading TOP SECRET Codeword," it is projected that these two texts might be written at the CONFIDENTIAL and SECRET levels respectively, to facilitate their handling and use in training programs. However, when the time actually comes for the preparation of these two texts it might be necessary to raise the classification of either one or both of them, dependent upon the treatment of the information contained. I disagree, however, with the apparent inference that the solution of codes and enciphered codes, for example, is automatically in the highest classification category because of the applicability of these techniques in operational problems. We have had for years CONFIDENTIAL training problems in enciphered-code solution in both known and unknown codes. In this connection, I might add that I have in my files a quite old paper (about 1930), on additive-enciphered code solution written by an amateur who had never been in the business; he described in great detail the use of differencing techniques, etc. There certainly seems to be a need for a common ground on such matters.

6. It would be interesting to have GCHQ views of the foregoing views and comments.

L. D. CALLIMAHOS