STANDARD FORM NO. 64

SECRET REF ID:A57374

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. W. F. Friedman DATE: 22 March 1954

FROM : Mr. L. D. Callimahos

SUBJECT: Security Classification of Training Materials

1. Reference is made to message "P 091446Z" from GCHQ to SLO Washington, addressed to Brigadier Tiltman from DD.

2. The British object to par. 6.54 of NSA-72's "Current Cryptanalytic Techniques" being included in a CONFIDENTIAL document. I can see no reason why any of the subparagraphs 6.54a through 6.54f merit a classification any higher than CONFIDENTIAL according to our standards. It is true that all of these subparagraphs have at one time or another covered operational systems; but is it also true that many portions of other cryptologic training texts, CONFIDENTIAL or unclassified, have or have had operational applicability.

3. 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?

4. As for the general statement in GCHQ's message 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 NSA-72 work and I cannot find anything which to our mind would warrant exclusion from the standpoint of a CONFIDENTIAL document.

5. In paragraph 4 of GCHQ's message is is stated that the syllabus of the Military Cryptanalytics series shows that "Parts I through IV are correctly graded CONFIDENTIAL since they are concerned with techniques that have repeatedly been described in published literature." Is it the British view, then, that items appearing in the public domain are automatically classified CONFIDENTIAL? It happens that Parts I-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 the classification of CONFIDENTIAL. As for the British complaint 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," what I have planned for Parts V and VI will include information at the CONFIDENTIAL and SECRET levels, respectively. However, when the time 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 British 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.

SECRET

Incl 2

Lambros D. Callimahos