~~TOP SECRET~~

D R A F T

12 September 1949

~~TOP SECRET - U.S. EYES ONLY~~

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

THE PROBLEM

1. To determine the U.S. Position toward the United Kingdom's proposals in RDC 5/99 (attached as Appendix "A") that:

(1) there be a full and complete interchange of cryptographic principles and policy on a reciprocal basis.

(2) if the U.S. Chiefs of Staff cannot agree to (1) above, they authorize the disclosure of the principles and details of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Of the two foregoing proposals, the first is unacceptable. The United States Government adheres to the generally accepted basic principle of national sovereignty and security that the means and methods which a government employs for the protection of its own communications constitute a private matter not to be shared in toto with any other government. This principle is sound because it is impossible to be certain that a former ally will not be someday over-run by a common enemy or may even become a foe, in which case a well-forged weapon may be turned against its originator. As regards the effects of such a contingency, the primary danger in the cryptologic field is not that the security of communications may be destroyed or impaired but that the sources of communication intelligence may be dried up.

3. With regard to the second proposal, it is felt that this solution to the problem should be accepted by the United States, for the following reasons:

a. In the spring of 1947 there were Joint and Combined conferences on this subject. At the Joint conferences the Army representatives favored disclosure of the ECM principles to the British for incorporation in a new CCM but in deference to Navy objections it was finally jointly agreed not to make such disclosure. At the Combined conferences it was decided to initiate studies which might lead to improvements in the security of the CCM. The results of these studies have been largely negative, the only improvements found to be capable of practical embodiment being those incorporated in a modification of the CCM known as the BCM (CSP 3800). However, the increase in crypto-security afforded by the BCM over that afforded by the CCM is not deemed to be of a sufficient degree to warrant U.S. insistence on British acceptance of the BCM as a long-term replacement for the CCM. Moreover, the modifications which would be required in the British Typex machine to convert it into a BCM are such that U.S. technicians are doubtful that they are practicable. Also, the British have decided that they must replace the Typex in any case and the introduction of a suitable replacement would be expensive in terms of time required for research, development, and service testing. It would be to the advantage of the U.S. as well as to the British if such a delay could be avoided so that British equipment suitable also for Combined Communications would become available at an early date.

b. During the Combined discussions referred to above, the British indicated that they were aware of the principles of the ECM. They described them quite accurately and indicated that they considered their security to be of the highest order. They admitted, in fact, that they had incorporated those cryptographic principles in a radioteletype cipher machine for their own use. Furthermore, even as regards the engineering know-how which went into the construction of the ECM, this knowledge has been disclosed to the British, since they were provided

with CSP 1700, a machine which is simply an ECM chassis with certain of the ECM cryptographic features eliminated.

c. Disclosure of the ECM to the British and its adoption by them would give the two governments a suitable piece of equipment ensuring the highest degree of security for vital combined U.S. - British communications on a long-term basis.

d. Disclosure of the ECM will not leave the U.S. without unique crypto-equipment. As a matter of fact, a modification of the ECM has already been developed (CSP 2900) and is available in quantity. This modification, which improves the security of the ECM, does so without in any way impairing its use as an ordinary ECM or as a CCM. By means of a simple switching arrangement it is possible to make the CSP 2900 serve as a device purely for U.S. communications, or as an ECM for U.S. - British combined communications, or as a CCM. However, the principles of the CSP 2900 would not be disclosed to the British.

e. Release of the ECM to the British would leave the way open to the adoption of the CCM for North Atlantic Pact communications if such a decision should be found to be necessary in the national interest. British - U.S. use of the ECM would be easily adaptable to North Atlantic Pact communications since the addition of a simple already available adapter to either the ECM or the CSP 2900 would permit communication with any North Atlantic Pact nation holding the CCM. In addition, disclosure of the CCM to the other signatories to the North Atlantic Pact would not impair the security of U.S. - British communications since the CCM system would then be reserved for North Atlantic Pact communications.

f. At the time of the 1947 Combined discussions on this subject, one of the principal U.S. objections to disclosing the ECM to

the British was the increased danger of compromise arising from the wider distribution of the equipment if the British were permitted to have it. This increased danger is recognized but it is believed that the advantages cited above outweigh this objection.

g. Also at the time of the 1947 Combined discussions there were indications that the British did not provide and enforce physical security protective measures for their crypto-equipment equal to those required and enforced by the U.S. services. Because of this it was agreed on a Combined level that a prerequisite to further discussions regarding a replacement for the CCM would be a Combined agreement covering the measures both governments would apply in the handling and protection of combined cryptomaterial. Such an agreement has been concluded and concurred in by both Governments (CCB-285, 11 Oct 1948). A review of that document in order to insure identity in security regulations applicable to the ECM and an acceptance of such changes therein as may be deemed necessary by the U.S. should be a preliminary to entering upon discussions leading to a full disclosure of the ECM to the British.

CONCLUSIONS

4. It is concluded that:

a. The first proposal made by the United Kingdom in RDC 5/99 of 13 July 1949 should be rejected.

b. The details of construction of the ECM (SIGABA) should be disclosed to the U.K. in discussions which should be preceded by a review and acceptance by both Governments of identical security regulations to insure the physical protection and proper use of the equipment.

~~TOP SECRET~~

RECOMMENDATIONS

5. It is recommended that:

a. A memorandum substantially as in Appendix "B" be forwarded to the British Joint Services Mission.

COORDINATION

6. Coordination with AFCIAC has been effected.

~~TOP SECRET~~

E N C L O S U R E

BRITISH JOINT SERVICES MISSION
OFFICES OF THE COMBINED CHIEFS OF STAFF
WASHINGTON

RDC 5/99

REPLACEMENT OF THE PRESENT COMBINED CYPHER MACHINE

Previous References:-

RDC 5/87 - 18 May, 1949
SM-1041-49 - 6 June, 1949

1. The representative of the U.K. Chiefs of Staff have been instructed to put forward, for consideration by the U.S. Chiefs of Staff, the attached memorandum dealing with the replacement of the existing Combined cypher machine.

2. Commander Burton-Miller of the U.K. Cypher Policy Board is now in Washington and is fully authorized to discuss this matter. It is hoped, therefore, that a very early decision on the attached proposals may be given us.

/s/ R. D. COLERIDGE
Captain, R.N.

13th July, 1949

~~TOP SECRET~~

APPENDIX "A"

~~TOP SECRET~~

A P P E N D I X

BRITISH JOINT SERVICES MISSION IN WASHINGTON

REPLACEMENT OF THE PRESENT COMBINED CYPHER MACHINE

MEMORANDUM BY REPRESENTATIVES OF THE U. K. CHIEFS OF STAFF

1. The U.K. Chiefs of Staff have given further consideration to the enquiry put forward in RDC 5/87 of the 18th May and are of the opinion that the phrase "with a view to improving the present Combined Cyphering System" in paragraph 2 may not have conveyed to the U.S. Chiefs of Staff the full purpose of their enquiry. They have therefore asked that certain additional factors should be brought to the notice of the U.S. Chiefs of Staff.

2. These factors are:-

(a) The U.K. Chiefs of Staff have decided that they must replace their Main Cypher Machine (Typex) as soon as possible since they do not consider that it will offer adequate security in the near future;

(b) In view of the fact that the Royal Navy can only carry one machine in the smaller ships the new British machine must be such that it provides both for British and for Combined British - U.S. communications;

(c) The experts of both nations agree that the cryptographic principles employed in the present C.C.M. are not sufficiently secure for the Combined Communications of another emergency.

3. The U.K. Chiefs of Staff propose a full and complete interchange of cryptographic principles and policy on a reciprocal basis. They are convinced:-

(a) That only thus can the highest degree of security be ensured for vital combined U.S. - British communications;

(b) That such an exchange can be made without loss of National Security to either Nation.

~~TOP SECRET~~

4. If the U.S. Chiefs of Staff cannot agree to the proposal in paragraph 3 above, and if it is their intention to retain their present cypher machine, the U.K. Chiefs of Staff propose that the U.S. Chiefs of Staff should authorize the disclosure to the U.K. Cryptographers of the principles and details of the E.C.M. so that these may be incorporated in the new British machine.

5. The U.K. Chiefs of Staff point out that unless full collaboration in this field is authorized now, the development of the British machine may have advanced to the stage where modification to ensure secure Combined Communications will not be possible.

- - - - - - - - - -

13 July, 1949

JOINT COMMUNICATIONS - ELECTRONICS COMMITTEE

SECURITY AND CRYPTOGRAPHIC PANEL

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

(Proposed reply to the British Joint Services Mission)

1. The U. S. Joint Chiefs of Staff have carefully considered the proposals made in RDC 5/99 of 13 July 1949 concerning the replacement of the existing Combined Cipher Machine. The U.S. Joint Chiefs of Staff regret that they are unable to accept the proposal for a full and complete interchange of cryptographic principles and policy on a reciprocal basis. However, they are prepared to authorize discussions which can commence in Washington at any time, leading to the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine, these discussions to be preceded by a review and acceptance by both Governments of identical security regulations to provide for the physical protection and proper use of the equipment.

APPENDIX "B"