

~~TOP SECRET~~~~TOP SECRET U. S. EYES ONLY~~*This is the final
paper as adopted
by AFCIAC + then
by JCS.*

AFCIAC: 13/12

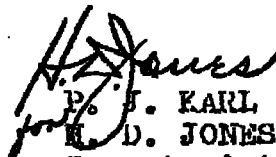
30 September 1949

MEMORANDUM FOR MEMBERS OF AFCIAC:

Subject: Replacement of the present Combined Cipher Machine.

1. The attached report of the Ad Hoc Committee, appointed by AFCIAC to prepare an amended reply to the British RDC/5/99 proposals, is forwarded for your information.

2. The Chairman, AFCIAC, has requested that your concurrence or comment be communicated to the SECRETARIAT at the earliest practicable date.



P. S. KARL
R. D. JONES
Secretariat, AFCIAC

Declassified and approved for release by NSA on 09-20-2013 pursuant to E.O. 13526

AFCIAC: 13/12

PRNC-NCSW-346

~~TOP SECRET~~

~~TOP SECRET~~D R A F T~~TOP SECRET U. S. EYES ONLY~~REPORT BY JOINT COMMUNICATIONS - ELECTRONICS COMMITTEETOJOINT CHIEFS OF STAFFREPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINETHE PROBLEM

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

a. There be a full and complete interchange of cryptographic principles and policy on a reciprocal basis.

b. If the United States Chiefs of Staff cannot agree to a. above, they authorize the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in the new British cipher machine (BCM).

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Appendix "C" (page 3)

CONCLUSIONS

3. a. It is not in the best interest of the U. S. to agree to the full and complete interchange of cryptographic principles with the British.

b. The release of the BCM under present circumstances is not warranted.

c. The details of the principles of the BCM should be disclosed to the U. K. with a view to its use as a replacement for the existing Combined Cipher Machine. In addition the U. S. should furnish to the U. K. on a continuing basis such improvements to the BCM as become available.

RECOMMENDATIONS

4. It is recommended that:

a. Memorandum substantially as in Appendix "B" be forwarded to the British Joint Service Mission.

COORDINATION

5. Coordination with AFGLAC has been effected.

Declassified and approved for release by NSA on 11-19-2013 pursuant to E.O. 13526

~~TOP SECRET~~

TOP SECRET~~TOP SECRET~~

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-1043-49 - 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-Filler 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.

13 July, 1949

~~TOP SECRET~~

APPENDIX "A"

TOP SECRET

~~TOP SECRET~~TOP SECRETTHE JOINT COMMUNICATIONS ELECTRONICS COMMITTEETHE SECURITY AND CRYPTOGRAPHIC PANELREPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

(Proposed reply to the British Joint Service Mission)

The U.S. Joint Chiefs of Staff have carefully considered the proposals made in RDC 5/99 of 13 May 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 the full and complete interchange of cryptographic principles and policy on a reciprocal basis. Full recognition, however, is accorded the view of the U.K. Chiefs of Staff regarding the necessity for the replacement of the present CCM for high level Combined use. In this regard the U.S. has developed and has in operation a machine (BCM) which is considered the best available equipment and entirely satisfactory for such communications. The BCM is relatively economical to manufacture and may be utilized in adaptor form with the present British basic cipher equipment, thus providing an economical as well as expeditious method for improving the security of combined communications. As an alternative proposal to the release of the ECM the U.S. will disclose to the United Kingdom the details and cryptographic principles of the BCM and will enter into discussions concerning its adoption for Combined use and concerning the physical security necessary for its protection. These discussions can commence in Washington at any time.

APPENDIX "B"

~~TOP SECRET~~

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

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. The United Kingdom Chiefs of Staff have decided that they must replace their main cipher machine (TYTEX) as soon as possible since they do not consider it will offer adequate security in the near future.

2. In view of the fact that the Royal Navy can carry only one machine in the smaller ships the new British machine must be such that it will provide for British and for Combined British and U. S. communications. This also applies in the United States Navy.

3. Although the CCM, if properly used, is a highly secure machine, the experts of both nations agree that the cryptographic principles employed in the machine are not as secure as is considered desirable for highest level United States - United Kingdom communications.

4. The United States government adheres to the general 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.

Because of the common interest of the U. K. and U. S. in world affairs today, the U. S. has a vital interest in the provision of a cryptographic system for Combined communications of assured security for highest level use. On the other hand the U. S. in its own national interest must reserve for itself a cipher equipment of assured security, to provide privacy for its own communications.

5. Because of financial limitations it is unlikely that the British are in a position to replace their present main cipher machine (TYTEX). Moreover, the United States should not, under the present circumstances, release the ECM if it is to adhere to the above stated policies, since the only equipment which might be considered to assure the necessary national privacy, the CSP 2900, will not be available in sufficient quantities to meet U. S. mobilization requirements for a considerable period of time.

6. The present BCM (CSP 3800) is sufficiently secure for highest level traffic, although not as secure as the ECM. The Navy has under development further modifications of the BCM which are expected to give it a security comparable to that of the ECM without incorporating any of the basic ECM principles. Design has already been completed for an adaptor which will permit the conversion of the TYTEX to a BCM.

~~TOP SECRET~~ Appendix "C"

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

7. Improvement of the security of Combined U. S. - U. K. communications can be most expeditiously achieved by release of the BCM to the British. The provision of this device will permit the British to continue the use of their basic cipher equipment modified by a relatively cheap and easy to manufacture adaptor. The same thing hold true insofar as the U. S. is concerned since an adaptor can be provided for the ECM-CSP 2900.

~~TOP SECRET~~