~~TOP SECRET~~

NATIONAL MILITARY ESTABLISHMENT
ARMED FORCES SECURITY AGENCY
Washington 25, D.C.

AFSA-11/ph
A6-3
Serial

D R A F T

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

MEMORANDUM FOR SECRETARIAT JCEC:

Subject: Replacement of the Present Combined Cipher Machine.

Reference: (a) CECM-940 dated 29 July 1949.

Enclosure: (A) Draft Staff Study dated 15 August 1949 (Subj: Replacement of the Present Combined Cipher Machine).

1. Enclosure (A) is forwarded in response to the request made in reference (a).

E. E. STONE
Rear Admiral, U.S.Navy,
Director, Armed Forces Security Agency

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

PRNC-NCSW-346

~~TOP SECRET~~

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 of 13 July 1949 for improving the security of Combined communications.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. The British Chiefs of Staff have proposed two possible solutions:

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

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

3. 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.

4. 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. This same point also applies in the U.S. Navy.

5. 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.

6. If a complete exchange of cryptographic principles and policy were to take place, the defeat or withdrawal of either nation could expose to compromise all cryptographic activity of the other.

7. If the principles of the ECM became known to any nation whose cryptographic systems now permit the obtaining of communication intelligence by the U.S., that nation could commence using the ECM for its communications, thereby greatly reducing the effectiveness of our communication intelligence effort.

8. There is in existence and operation, in the U. S. Navy, a cipher machine incorporating modification of the CCM principle. This machine is known as the BCM (CSP-3800). The security of the BCM has been evaluated as greatly superior to that of the CCM.

9. The disclosure to the United Kingdom of the details of the BCM will not provide the British with any cryptographic principles which they do not already know. The reverse stepping of the 2nd and 4th rotors represents a principle already incorporated by the British in their proposed machines RM26 and RM32. The change in order of progression represents a modification of the CCM principle which has already been specifically requested by the United Kingdom.

CONCLUSIONS

10. It is concluded that:

a. Both proposals made by the United Kingdom in RDC 5/99 of 13 July 1949 be rejected.

b. The BCM (CSP 3800) be offered to the British for use in its present form, or with such modifications as may be agreed upon, as a replacement for the existing Combined Cipher Machine.

RECOMMENDATIONS

11. It is recommended that:

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

COORDINATION

12. Coordination with AFCIAC has been effected.

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. While it has been agreed that discussions should take place with a view to improving the present system, the U.S. Joint Chiefs of Staff regret that they cannot agree to a full and complete interchange of cryptographic principles and policy on a reciprocal basis, nor can they authorize the disclosure of the principles and details of the ECM.

2. The U. S. has developed, and has in operation, a machine known as the BCM, which uses a modification of the CCM principles and which has much greater security than the CCM. Furthermore, the U.S. has under development improvements to the BCM which it is expected will increase the present security considerably. The U.S. Joint Chiefs of Staff are agreeable to disclosing to the United Kingdom the details and cryptographic principles of the BCM, and to entering into discussions concerning the use of the BCM or some modification thereof for possible future combined communications. If the United Kingdom desires to enter into such discussions, it would be convenient to the U.S. Joint Chiefs of Staff to begin these discussions in Washington in September 1949.

3. In the event that a machine superior to the CCM is adopted for combined use, the U.S. Joint Chiefs of Staff must require definite assurance that the utmost care will be taken in the physical protection of such a machine, and in accounting for it. While it is true that the security of traffic encrypted with any acceptable modern cipher machine should be unaffected by physical compromise of the machine or its general principles, it is considered fundamental that the greatest possible degree of physical security be maintained.