~~TOP SECRET~~

~~U.S. EYES ONLY~~

This is the 1st proposed reply – nonconcurrence from ASA. 3

AFCIAC: 13/3

29 August 1949

MEMORANDUM FOR MEMBERS OF AFCIAC:

Subject: Replacement of the Present Combined Cipher Machine.

Enclosure: Draft Memorandum for Secretariat, JCEC, subject as above.

1. The enclosure represents a revision of the paper AFCIAC: 13/1 dated 16 August 1949, and is circulated herewith for telephonic concurrence as a matter of priority.

2. Attention is invited to the fact that this revision was made as a result of comments and recommendations received after AFCIAC 13/1 was circulated for vote. This revision makes no substantial changes in the position of the U.S. on the subject matter, and aside from making editorial changes, a few additional facts bearing on the problem have been added.

P. J. KARL
for H. D. JONES
Secretariat, AFCIAC

cc: Captain H. O. Hansen, USN
Dr. A. Sinkov

AFCIAC: 13/3

~~U.S. EYES ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

NATIONAL MILITARY ESTABLISHMENT

ARMED FORCES SECURITY AGENCY

Washington 25, D.C.

AFSA-11/
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 24 August 1949 (Subj: Replacement of the Present Combined Cipher Machine).

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

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

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

~~TOP SECRET~~

~~TOP SECRET~~

AUG 24 1949

D-R-A-F-T

~~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 of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. 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.

3. 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 also applies in the U.S. Navy.

4. 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 the highest level U.S. - U.K. communications of another emergency.

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

Substitute new par. 5.

~~TOP SECRET~~

D R A F T

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

6. 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 reducing the effectiveness of our communication intelligence effort. It is for this reason that the U.S. services have withdrawn the ECM from sensitive areas and replaced it by the present CCM.

7. Several instances of loss of the CCM by British holders have occurred. These indicate that British commands have not provided for cipher machines physical security equal to that deemed necessary by the U.S. Services.

8. Present U.S. Policy regarding disclosure of the ECM reads, in part, as follows:

> "The U.S. Army and Navy mutually agree that they will regard as secret information to be divulged only to the armed forces of the U.S. or to any U.S. citizen required to possess this information in the interests of the United States, any details concerning the ECM-M134C including rotors, wiring diagrams, keys, keying instructions and operating instructions. If at any time either the Army or the Navy considers it necessary to deviate in any way from this policy, the one shall fully inform the other of the facts and circumstances and the change in policy, if any, shall be by joint agreement."

Level 7

9. This agreement was jointly approved on 26 June 1942, at which time the Air Force was part of the Army. There appears to be no reason at this time for any change therein.

9. The Armed Forces of the United States must reserve for themselves, for reasons of privacy and security, at least one high-level system. The only such system presently available in sufficient quantity is the ECM.

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

10. There is in existence and operation, in the U.S. Navy, a cipher machine incorporating modification of the CCM principles. 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, and as entirely suitable for the highest level communications.

CONCLUSIONS

11. It is concluded that:

a. Present U.S. policy does not permit disclosure of the principles of the ECM to the United Kingdom and is justified in view of U.S. experience with British physical security practices.

b. A modification of present policy is not warranted.

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

d. The details and principles of the BCM (CSP 3800) should be disclosed to the U.K.

e. Discussions should be held with the U.K. concerning the adoption of the BCM for combined use, either in its present form or with such modifications as may be agreed upon, as a replacement for the existing Combined Cipher Machine.

RECOMMENDATIONS

12. It is recommended that:

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

COORDINATION

13. Coordination with AFCIAC has been effected.

TOP SECRET

~~TOP SECRET~~

ENCLOSURE

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~~

TOP SECRET

APPENDIX "A"

~~TOP SECRET~~

APPENDIX

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

~~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

~~TOP SECRET~~

TOP SECRET

~~TOP SECRET~~

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, and regret that they are unable to agree to either of the proposals. Full recognition, however, is accorded the view of the U.K. Chiefs of Staff regarding the necessity for replacement of the present CCM for high-level combined communications. In this regard, the U.S. has developed, and has in operation, a machine (BCM) which is a modification of the CCM and which the U.S. considers ~~considered entirely~~ satisfactory for such communications. If the U.K. Chiefs of Staff desire, 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.