~~U.S. EYES ONLY~~
~~U. S. EYES ONLY~~

AFSAC: 13/40

19 June 1950

MEMORANDUM FOR MEMBERS OF AFSAC:

Subject: Replacement of the Present Combined Cipher Machine (CCM).

1. The subject paper is enclosed herewith, and has been placed on the Agenda for consideration at the Fifteenth Meeting to be held on 19 June 1950.

J. W. PEARSON
H. D. JONES
Secretariat, AFSAC.

AFSAC: 13/40

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

REF ID:A2435986

REPORT BY THE ARMED FORCES SECURITY AGENCY COUNCIL

VIA THE JOINT COMMUNICATIONS-ELECTRONICS COMMITTEE

to the

JOINT CHIEFS OF STAFF

on

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE (CCM)

Reference: J.C.S. 2074 Series

THE PROBLEM

1. To draft, for approval of the Joint Chiefs of Staff, a reply to the memorandum by the Representatives of the British Chiefs of Staff, RDC 1/46 dated 14 February 1950 (JCS 2074/3) regarding the feasibility of constructing an adaptor for U.S. use which will permit intercommunication with the contemplated new British cipher machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B".

CONCLUSIONS

3. It is concluded that:

a. While there is no doubt that the British are aware of the basic important ECM principles, and propose to incorporate them in a new British cipher machine, they apparently lack considerable detailed knowledge concerning our specific application of these principles in the ECM.

b. To adapt the proposed British cipher machine to use for U.S.-U.K. combined communications appears to be feasible, provided the U.S. reveals to the British the detailed information concerning the ECM which they now lack, and would require to produce a machine practically equivalent to our ECM.

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

c. The replacement for the CCM, to be agreed upon by the U.S.-U.K., may later, especially in wartime, have to be used also by allied British Dominions, particularly Canada, and possibly by other allied countries.

d. The U.S., as a matter of policy, should not disclose to any foreign country the complete details of the ECM, even though technical considerations might favor the use of the ECM for combined communications.

e. While the proposed British cipher machine would be adequately secure for highest-level communications, development, refinement and procurement of such a machine by the agreed date for replacement (1 January 1955) is extremely doubtful.

f. The U.S. has current need, without considering combined needs, for more than one cipher machine affording adequate security for highest level communications.

g. The U.S. should propose to disclose to the British experts a working model of the 7-rotor BCM for consideration as replacement for the present CCM, in lieu of further consideration of adapting the contemplated British machine for combined U.S.-U.K. use.

h. The U.S. should also disclose to British experts a working model of the PCM when available.

i. In addition to a replacement for the present CCM, the U.S. and British Navies have an urgent requirement in combined communications for a secure small cipher machine - particularly for submarines, certain surface ships, and for large fast merchant ships.

j. Comparable British and U.S. cipher machines, whenever practicable, should use physically interchangeable rotors.

RECOMMENDATIONS

4. It is recommended that:

a. No further consideration be given to using the ECM principle for combined communications.

b. 7-rotor BCM and lightweight version, PCM, working models be disclosed in Washington by the U.S. to the British for consideration as the replacement for the CCM.

c. The U.S. reply to the British be as set forth in Enclosure "A".

ENCLOSURE "A"

MEMORANDUM FOR THE REPRESENTATIVES OF THE BRITISH CHIEFS OF STAFF

1. The U. S. Chiefs of Staff have had a thorough study made of the drawings of the proposed new British cipher machine which were submitted as an enclosure to RDC 1/48 of 12 April 1950. It has thus been ascertained that the proposed new British machine should be secure for highest level communications, and that a U. S. cipher machine probably could be adapted to permit intercommunication. However, a working model would be required in order to determine the practical feasibility of such adaptation.

2. Because of the time which experience indicates is required to develop, refine, and procure a new cipher machine, such as the U.K. has proposed, and because of important technical and policy considerations, instead of further considering the adaptation of the proposed new British machine, the U. S. Chiefs of Staff propose that as the long-term solution of a replacement for the present combined cipher machine (CCM), consideration be given to the 7-rotor BCM.

3. The U. S. now has a working model of a 7-rotor BCM available for examination in Washington by British cipher machine experts, if the British Chiefs of Staff are willing to consider the adoption of such a machine as replacement for the CCM. The U. S. expects also to have available for examination a smaller lighter-weight working model of the 7-rotor BCM (termed the PCM) before the end of calendar year 1950. This machine has been developed primarily for future Naval use. The 7-rotor BCM/PCM can readily be adapted to intercommunicate with the present CCM.

4. The U. S. 7-rotor BCM/PCM proposal for combined U.S.-U.K. communications has taken into consideration the necessity not only for providing security for highest-level command combined communi-

cations, but also for communications in combined operating forces. The U. S. Chiefs of Staff concur with the British Chiefs of Staff in wishing to avoid having numerous operating units (especially ships) encumbered with more than one type of cipher machine.

5. The security to be afforded by the 7-rotor BCM (PCM) is considered to be of about the same high order as the U. S. ECM and the proposed new British machine.

6. The U. S. Chiefs of Staff further propose that, so far as practicable, comparable British and U. S. cipher machines use physically interchangeable rotors. The 7-rotor BCM rotors are of the same size as those in the CCM (CSP 1700). Such standardization would permit emergency issue of rotors by either country to the other, if necessary.

7. If the U.S.-U.K. agree on the 7-rotor BCM (PCM) as the new combined cipher machine, the U.K. would not have to undertake extensive time-consuming development work, and, if desired, could probably expedite procurement by combining procurement orders. It is anticipated that the replacement date (1 January 1955) can be met if the 7-rotor BCM (PCM) is agreed upon as the replacement for the CCM; the 7-rotor BCM (PCM) would be less complex in construction than the proposed British machine, and most of the parts have already proven satisfactory in actual use.

~~TOP SECRET~~ REF ID: A2435986

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. While this paper pertains to U.S.-U.K. communications, it should be understood that the combined cipher machine to be agreed upon for U.S.-U.K. communications may later have to be made available for use also by allied British Dominions, especially Canada, and possibly also by other allied countries.

2. In JCS 2074, one of the conclusions of the U.S. Joint Chiefs of Staff was, "the release of the ECM under present circumstances is not warranted." Instead, JCS 2074 proposed, for combined use, a U.S. machine, the 5-rotor BCM. This machine was subsequently disclosed to the British and rejected on the grounds that a 5-rotor cipher machine would not be sufficiently secure as a long-term solution.

3. In RDC 5/99 dated 13 July 1949, the British Chiefs of Staff continued to express concern regarding the security of the present combined cipher machine on a long-term basis and stated:

a. That they had decided to replace their main cipher machine (TYPEX) as soon as possible.

b. That they felt it necessary to have a single machine which would be able to provide both intra-British communications and combined U.S.-British communications.

c. That they requested the U.S. Chiefs of Staff to authorize the disclosure to the U.K. cryptographers of the principles and details of the ECM so that these might be incorporated in the contemplated new British machine.

4. In JCS 2074/2 dated 10 January 1950, the U.S. Chiefs of Staff denied the British request for principles and details of the ECM, but indicated two possible alternative solutions:

a. Solution A. Disclosure by the U.K. of a copy of its contemplated new cipher machine, or detailed drawings thereof, so that the U.S. could ascertain the feasibility of constructing an adaptor for U.S. use which would provide the basis for secure combined communications by utilizing the new British machine, when available, and an existing U.S. machine with an adaptor.

b. Solution B. The possibility of using a 7-rotor BCM which the U.S. was developing.

These alternative solutions are discussed in paragraphs 5 and 6 below.

5. SOLUTION A:

a. The drawings of the contemplated new British cipher machine (Enclosure to JCS 2074/4 dated 13 April 1950) have been received and confirm the statement of the British Chiefs of Staff in Para. 6(b) of RDC 1/36 (Enclosure to JCS 2074/1, dated 6 December 1949) that the new British machine would be built to operate on the broad principles of the ECM.

b. The British security evaluation of their contemplated new machine is sound; the resistance of the machine to cryptanalysis should be at least as great as that of the ECM and hence would be adequately secure for highest-level communications.

c. It can be deduced from the drawings that the U.K. has not yet built a working model of the new British machine, and, therefore, while the U.K. still has full latitude in the determination of certain details of basic construction, it is several years away from the procurement stage.

d. Although the contemplated new British machine will embody the basic principles of the ECM, there are significant differences in detailed application of the ECM principles. As a consequence, in order to make the two machines intercommunicable, it would be necessary for the U.S. to provide the British with certain detailed information applicable specifically to the ECM.

e. The provision to the British of detailed information about the ECM would not be necessary for the use of their new machine for purely British intra-communication.

f. If the British are provided with required detailed ECM information, the security of the resulting combined system would be of the same high order as that of the ECM.

g. As regards the effects on our own communication security, of the disclosure to the British of the detailed information

referred to above, there probably would be no change in the security evaluation of the ECM. Although the U.S. has always emphasized the importance of the physical security of our cipher machines, our evaluation of the ECM is predicated on possible ultimate enemy possession of the ECM machine, and our security is based upon regularly changing the rotors and key lists. The privacy of U.S. communications against cryptanalytic attack by any foreign power, including the British, could be assured.

h. If the British were to include in their new machine appropriate wiring, based on detailed ECM information supplied by the U.S., security for intra-British communications would not be affected, and if certain special rotors were used by them, a relatively simple method of use of the ECM by the U.S. with one special rotor per machine would permit inter-communication between the proposed new British machine and the U.S. machine.

i. The cost to the U.S. of the adoption of this solution would be less than $1,000,000 and an existing U.S. machine (ECM) could be used for U.S.-U.K. combined communications.

j. Present U.S. procedure in the use of the ECM could remain unchanged, except for use of a special adaptor rotor.

k. The U.K. would have to use at least four special adaptor rotors, which would very slightly reduce the security of the British machine, but not sufficiently to cause any concern.

l. The great disadvantage of Solution A would be the loss of the full control of the ECM which we have always regarded as vitally important to the U.S.

6. SOLUTION B:

a. A model of the 7-rotor BCM is now available and can be shown to the British experts in Washington with a view to holding discussions regarding its adoption for combined communications. In this connection, certain points should be considered -- namely:

(1) The British desire to provide but one cipher machine for their own internal use as well as for combined use.

(2) We can adapt the ECM to work with the 7-rotor BCM, and the 7-rotor BCM to work with the present CCM. The present CCM will probably be in use for several years to come -- even though the U.S. and U.K. replace the present CCM for combined U.S.-U.K. use.

(3) A 7-rotor BCM should assure the U.S.-U.K. of the highest-level communications security on a long-term basis.

b. JCS 2074 stated that the means and methods employed for the protection of U.S. communications constitute a private matter not to be shared in toto with any other government, and that the U.S. must reserve for itself a cipher equipment of assured security to provide privacy for its own communications. Although it is now clear that the British understand the basic important principles of our ECM, and intend to incorporate them in their new machine, they lack important specific information concerning applications of these principles. As a matter of National policy, it is therefore considered proper not to disclose further details of the ECM to any foreign country.

c. Continuation of this policy appears desirable for the reason that by sharing the ECM, we lose much of the existing full control over this vital machine. Such full control:

(1) Permits us to enforce measures to insure the physical security of all elements of the machine against loss or compromise, by limiting distribution and prescribing adequate safeguards.

(2) Permits us full freedom to apply modifications when desired to enhance our communication security.

(3) Affords us maximum assurance that no foreign nation that might try to read our messages will have possession of one of our machines, which possession might permit a more direct attack (by cryptanalysts) by revealing details or modifications not already known. However, our cryptanalysts believe that such attack would not be successful unless the foreign nation concerned possessed also our rotors and key lists, which are regarded as more vital security elements than the machine chassis.

d. Experience to date indicates that neither the British nor the U.S. can develop, refine and produce a reliable completely-new cipher machine in less than five years. Therefore, the U.S. will probably have to offer the British a U.S.-developed cipher machine if the target date of 1 January 1955, which has been agreed upon as the replacement date for the present CCM, is to be met.

e. It is believed that the British, when shown a working model of the relatively less complex but highly secure 7-rotor BCM, will abandon their own proposed development and will accept the 7-rotor BCM as the replacement for the present CCM as well as for their own intra-British use. It can surely be refined and produced in less than five (5) years, if funds therefor are provided, (approximately $6,000,000 for the U.S.) because most of the parts have already proven satisfactory in actual use.

f. In addition to the problem of improving the security of highest-level combined communications, there is the current problem of providing improved, adequately-secure crypto systems for U.S. and U.K. operating force use, especially in:

(1) Merchant ships.

(2) Amphibious craft.

(3) Submarines.

(4) Patrol craft.

g. Since 1944 the U.S. Navy has had under development a small lightweight cipher machine (the PCM) to fill Navy requirements. The PCM will be cryptographically identical with the 7-rotor BCM, and should be suitable for large and small ships. It is expected that the first development model of the PCM will be completed about November 1950. Both the PCM and 7-rotor BCM will have provision for intercommunicating with the present CCM and ECM.

h. The logistical problem of secure combined communications is of much greater magnitude and complexity for the Navies concerned than for the respective Armies and Air Forces. For example, during World War II, the U.S. Navy procured and used about 15 times as many CCMs as the U.S. Army and Air Force combined, even though the CCM distribution was limited to "Major War Vessels" (destroyers and larger).

7. FACTS APPLICABLE TO BOTH SOLUTION A AND SOLUTION B:

a. A machine of improved security would have to be issued to those U.S. commands from whom the ECM was withdrawn in 1947 in sensitive overseas areas.

b. The effect upon the communication intelligence interests of the U.S. either during the present world situation or during actual hostilities, would be the same. If used by a foreign country, either proposed machine, for all practical purposes, would be unbreakable by the U.S.

c. Experience has demonstrated that the emergency issue of rotors by one country to the other is of considerable practical value. If British machines are designed to use the same size rotors as those used in comparable U.S. machines, such emergency issue would be greatly facilitated.

d. Although the cost to the U.S. in solving the immediate high level combined problem would be substantially larger under Solution B, the total over-all cost to the U.S. Government (particularly because of the special Naval requirements referred to in Paragraph f., which are combined as well as intra-U.S. Navy requirements) would be essentially the same under either solution. This total cost cannot be closely estimated pending completion of certain cipher projects still under development.

e. The U.S. has already agreed that, if necessary, we will provide the British with a limited number of adequately-secure cipher machines (from U.S. stocks) to meet an emergency situation which might arise before 1 January 1955 when the replacement CCM is to be available. Which U.S. machine this will be depends upon the then-existing circumstances.