AFSA-14

AFSA-00/wn
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

~~TOP SECRET - U. S. EYES ONLY~~ 12 December 1949

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

MEMORANDUM FOR DIRECTOR, COMMUNICATIONS-ELECTRONICS:

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

Reference: (a) JCS 2074 and 2074/1.

1. The Director, Armed Forces Security Agency is in receipt of a copy of JCS 2074/1, and has given preliminary consideration thereto. It is understood that this matter is now under consideration in JCEC and will be coordinated with AFSAC.

2. The conference with the British Cryptographic experts was conducted by the Director, Armed Forces Security Agency and his experts. The present views of the Director, Armed Forces Security Agency, together with other pertinent information, are set forth herein for possible assistance to the members of the JCEC and AFSAC in consideration of JCS 2074/1 and in preparing the required answer to the British.

3. The British assumption of a target date 5 years hence when we can and should have a new combined cipher machine seems valid. If necessary, in the event of an emergency before the completion of a new combined cipher machine, the U.S. might furnish (in limited numbers) a suitable secure U.S. machine to the U.K. for US-UK "high command" communications, and possibly also to certain Dominions, and perhaps to other allied countries, for the same type of communications. The machine suggested by the British as the long-term solution (7-rotor BCM) is a current development project. The first model has not yet been completed. It would be advantageous to the U.S. not to name at this time the specific machine we would make available when such an emergency arises. Today it might be a particular machine, and ten years hence a different one. However, we could -- and I think we should -- assure the British on this matter, in a general way. We agree with the British that a 7-rotor BCM should give adequate security for high command US-UK communications. It will take considerable money to

AFSA-00/wn
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

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

12 December 1949

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

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

produce it in quantity. The importance of secure US-UK communications is such that an adequate cryptographic machine must always be available. I believe that, as at present, it should be different from our own best machine for reasons stated hereinafter, and that it can be different with adequate security.

4. The U.S. does not have under development a 7-rotor CCM; furthermore, there appears to be no need for undertaking such a development at this time. The CCM, especially the model (CSP 2900) with certain modifications, is regarded as satisfactory and secure for highest level communications. We also have a limited number of another (more complex) modified CCM (CSP 2300) which is also regarded as secure for highest level communications. However, because of its complexity, it is not expected that there will be any further production of this machine. The CSP 2300 and 2900 are basically the World War II type CCM plus improvements to enhance security. The improvements were logical developments applied to the basic CCM and should not, therefore, be considered to have resulted in creating new type machines.

5. The British state that the CCM (World War II version of the basic CCM) was disclosed to them in 1942. A limited number of Britishers have seen it. They do not, however, have enough information to build a duplicate of our CCM. The British probably could construct a machine resembling our CCM. It probably would take them many years to do so, since our CCM has been about 30 years in the making. In private conversation the British admit they do not have an CCM blueprint. The CCM is necessarily a complex machine, and some of the details could not be ascertained by merely seeing it in operation. The only improved machine for our own use that we can now be sure of having is the modified CCM. Although we have some promising research and development

AFSA-00/wn
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

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

12 December 1949

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

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

projects in the cryptographic field, it will be several years more before we can expect to have a new U.S. cryptographic machine, based on different principles, and in sufficient quantity for regular U.S. use.

6. The British assumption that theoretically they could solve any 5-rotor machine is based on having a set of the rotors and a 25 letter "crib". Getting the rotors and crib might delay a start on such a solution indefinitely, and the result of each solution probably would be good for the traffic of but one day. Such an attack is theoretically possible, but to apply it to the 5-rotor BCM would require considerable time and much machinery (even if the rotors and crib are available). It would be an extremely difficult and costly undertaking. A 7-rotor BCM, if developed, would probably preclude such an attack. Attack on the basic ECM would be even more difficult than on the 5-rotor BCM, but theoretically possible. It must be assumed that what men can make, other men should be able to take apart. Practically, the risk of solution is considered small in either case.

7. I would especially invite attention to the Facts Bearing on the Problem as originally studied, and to the Discussion, in Enclosure "C" of JCS 2074. The content of that enclosure is still considered to be sound.

8. The United Kingdom's proposal to effect complete interchange of cryptographic principles on a reciprocal basis is still considered unacceptable. However, certain limited interchange on the other aspects they now propose is considered desirable on a conference basis, but not necessarily on a continuing basis. After the first such conference, with disclosure of such currently available developments by each side as are previously

AFSA-00/wn
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

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

12 December 1949

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

agreed upon, consideration could be given to the matter of future conferences and possibly to future collaboration.

9. We should inform the British that if they have or build a new cipher machine which they might care to disclose to the U.S. as a possible combined cipher machine, we would be pleased to consider it for such use in the future -- either by our building an adaptor for one of our own cipher machines, or, if that should not be feasible, then by building or buying the number of machines required by the U.S. for US-UK communications.

10. The U.S. should continue to develop a 7-rotor BCM and when a model is ready (expected within a few months) allow the U.K. to examine the principles of that machine. If both the U.S. and U.K. representatives agree that such a machine will be practical and adequately secure in use for twenty years after production, then agree to the adoption of the 7-rotor BCM for US-UK high command communications as the replacement for the present combined cipher machine.

11. The three proposals listed in paragraph 7 of Appendix to JCS 2074/1 are not feasible at this time. However, concerning the present CCM, paragraph 8 of Appendix to JCS 2074/1 is generally concurred in, since the CCM probably must be continued in use for several years for US-UK communications. The three steps proposed by the British to enhance the security of US-UK communications with CCM are admittedly desirable, and some or all of them may be practicable and in that case probably should be adopted.

12. For reasons briefly set forth below, the Director, Armed Forces Security Agency believes that it should continue to

AFSA-00/wn
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

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

12 December 1949

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

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

be U.S. policy not to give any foreign nation our most secure cryptographic machine, or the principles thereof. Such action is not necessary to insure secure US-UK communications. The primary objections are as follows:

a. Twenty or thirty years from now, the U.S. may still be depending upon the CCM (or a modified CCM) for security of its own communications.

b. From the political viewpoint -- no one can foretell what kind of Government will be in control of any foreign country twenty or thirty years hence, or what our relations with such a country then will be. Of course, it is to be hoped and expected that they will be friendly in the case of the U.K. and the Dominions.

c. Giving the CCM to any foreign country removes the sole control and custody of that machine from the U.S.

(1) We could not as readily apply modifications which we might consider essential for our own or for combined use.

(2) There are three important physical security aspects of any machine, and none of them should be ignored: namely, the basic machine, the rotors, and the key lists. We could not be sure that adequate physical security would be given to our basic machine to prevent loss or capture, even though our communications should be secure so long as the rotors and key lists are not compromised.

(3) We could not be sure that our machine would not be used in places or in types of ships or

AFSA-00/wm
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

~~TOP SECRET - U.S. EYES ONLY~~ 2 December 1949

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

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM)

airplanes where we ourselves would not permit such machines to be used -- combined agreements to the contrary notwithstanding.

(4) It probably will be essential to extend the use of any machine agreed upon for combined communications to more than one allied foreign country: e.g., to Canada, Australia, or possibly even to the French, Dutch, etc.

13. With the consideration I have been able to give this extremely important problem to date, my views as to an answer to the British are as follows:

a. Agree that US-UK communications must continue (probably for five years if no emergency should develop in that period) to be by present CCM - but made more secure, if possible, by use of new and additional rotors and key lists and by minor material improvements -- until a new combined cipher machine is available for US-UK and Dominion use.

b. Propose that the U.S. continue to develop a 7-rotor BCM as a probable replacement for the present CCM for combined use. Both U.S. and U.K. experts already have agreed that such a machine should insure the necessary security for the next 20 years. The cost to the U.S. will be considerable but necessary. This proposal, if agreed to, would have the one vitally important advantage of retaining the CCM (and such modified CCM as we may hereafter use for U.S. communications) exclusively for U.S. use, and assurance of sole U.S. control and sole U.S. physical custody. The decision about combined use should be

AFSA-00/wm
A6
Serial: 00040

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D.C.

~~TOP SECRET - U.S. EYES ONLY~~ 12 December 1949

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

SUBJECT: Replacement of the "Combined Cipher Machine" (CCM).

made only after a 7-rotor BCM model has been examined and approved by both U.S. and U.K. representatives.

c. The U.S. should agree to make available to the British in an emergency, a secure cipher machine in limited numbers to meet initial urgent combined US-UK needs. Although this conceivably might be the World War II version of the ECM, it could be the 5-rotor BCM, or some other machine then available and sufficiently secure. It is considered neither necessary nor wise to mention at this time the specific machine. We should reserve the right to make that decision if and when required, based upon the circumstances then existing.

/s/ EARL E. STONE
REAR ADMIRAL, U.S. NAVY
DIRECTOR, ARMED FORCES SECURITY AGENCY

Copy to:

Members of AFSAC

AFSA-00A
AFSA-00B
AFSA-00C
AFSA-11S
AFSA-04
AFSA-14
AFSA-001