

AFSAC: 66/46

24 December 1952

TOP SECRET - SECURITY INFORMATION

MEMORANDUM FOR THE MEMBERS OF AFSAC:

Subject: Replacement of the Combined Cipher Machine.

The inclosure is forwarded for your information.

*M. C. Fisher*

M. C. FISHER  
LTJG, USN  
Secretary, AFSAC

Inclosure - 1  
Memo for Secretary, JCS,  
dtd 23 Dec 52, Serial - 000417

(less incl)

AFSAC: 66/46

~~TOP SECRET~~

NATIONAL SECURITY AGENCY  
Washington 25, D. C.

Serial: 000417

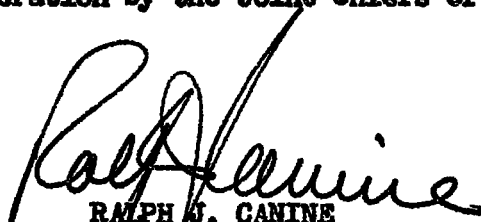
23 December 1952

TOP SECRET - SECURITY INFORMATION

MEMORANDUM FOR THE SECRETARY, JOINT CHIEFS OF STAFF

SUBJECT: Replacement of the Combined Cipher Machine

The inclosure is forwarded, in accordance with  
SM-2788-52, for consideration by the Joint Chiefs of  
Staff.

  
RALPH S. CANINE  
Major General, US Army  
Director

Incl:

Memo by DIRNSA for the  
JCS, subj. as above

cc: DDI (2)  
DDS (1)  
CONS (1) ←  
C/S (1)  
AG (1)  
P/P (2)  
LOG (1)  
R/D (2)  
C/SEC (3)

M/R: Self-explanatory.

Col. A.L. Pachynski, Comsec,  
Ext. 501

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
Copy 24 of 35 copies  
Page 1 of 1 pages

~~TOP SECRET~~

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM BY THE DIRECTOR, NATIONAL SECURITY AGENCY

for the

JOINT CHIEFS OF STAFF

on

REPLACEMENT OF THE COMBINED CIPHER MACHINE

- References: a. J.C.S. 2074/9
- b. J.C.S. 2074/14
- c. J.C.S. 2074/21

1. The U.K. Chiefs of Staff have replied (Enclosure to J.C.S. 2074/21) to proposals made by the U.S. Joint Chiefs of Staff (Enclosure "A" to J.C.S. 2074/14) pertaining to replacement of the existing Combined Cipher Machine (CCM). The proposals by the U.S. Joint Chiefs of Staff were made in light of a request by the U.K. Chiefs of Staff, dated 4 January 1952 (Enclosure to J.C.S. 2074/11), for the U.S. to provide equipments (either AFSAM 7 or AFSAM 47) on a free loan basis for Commonwealth and NATO use, regardless of whether the cryptoprinciple was ADONIS or BRUTUS. The U.K. Chiefs of Staff now urge selection of the BRUTUS system to replace the CCM in accordance with a UK/US agreement, made in September 1950 and approved by the U.S. Joint Chiefs of Staff in July 1951, to use this cryptoprinciple (Enclosure "B" to J.C.S. 2074/9).

2. The reply to the U.K. Chiefs of Staff contained in the enclosure confirms the urgency of the problem and recommends that a final agreement be reached on the cryptoprinciple for the new Combined Cipher Machine. This approach to the problem avoids comparisons of specific equipments, not all of which are sufficiently advanced for such comparison, but opens the way for prompt and concerted action by both the U.S. and U.K. for replacing the CCM by ending vacillation in the making of a choice between two strong cryptoprinciples. The reply recommends that the ADONIS cryptoprinciple be agreed upon, lists the advantages which it offers operationally and logistically, and presents a practicable means of implementing it.

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
 Copy 24 of 35 copies  
 Page 1 of 6 pages

~~TOP SECRET - SECURITY INFORMATION~~

3. Separate action will be taken later with respect to the question of release of the new Combined cryptoprinciple to the Union of South Africa raised in Enclosure "B" to JCS 2074/21 (ACT 97).

4. It is recommended that the draft memorandum in the Enclosure be forwarded to the Representatives of the U.K. Chiefs of Staff.

TOP SECRET CONTROL NUMBER 52-1534  
Copy 24 of 35 copies  
Page 2 of 6 pages

~~TOP SECRET - SECURITY INFORMATION~~

ENCLOSURE

DRAFT

MEMORANDUM FOR THE REPRESENTATIVES OF THE UNITED KINGDOM CHIEFS OF STAFF

Subject: Replacement of the Combined Cipher Machine

1. The magnitude and complexity of the program for replacing the present Combined cryptoprinciple LUCIFER with a new principle, particularly when it is extended to NATO, makes it essential that our agreement be based on objective consideration of total cost, total production capabilities, total logistical support, and long-term security. With these considerations in mind, the United States Joint Chiefs of Staff have studied the United Kingdom Chiefs of Staff memorandum ACT 96, dated 5 December 1952, and regret that they cannot agree to the proposals in paragraph 6 thereof.

2. The U.S. Joint Chiefs of Staff agree as to the urgency and importance in reaching agreement on this problem. Further delays can be avoided by our making a firm and final decision as to the cryptoprinciple to be employed in the new Combined Cipher Machine. This will then permit our respective technical organizations to take rapid, concerted, and simultaneous action to obtain the equipment which embodies the agreed principle. Accordingly, the U.S. Joint Chiefs of Staff propose that:

- a. The cryptoprinciple ADONIS be designated as the new Combined and NATO cipher system;
- b. The United Kingdom and United States jointly prepare a plan for the phased introduction of ADONIS to begin on 1 January 1955.
- c. The U.S. make available to the U.K., under arrangements to be determined later, U.S. ADONIS equipments until such time as the U.K. can provide for its own version of ADONIS.

Enclosure

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
Copy 24 of 35 copies  
Page 3 of 6 pages

~~TOP SECRET - SECURITY INFORMATION~~

3. Agreement on the adoption of ADONIS is urged for the following reasons:

a. The United States Joint Chiefs of Staff consider that 36-point wired rotors used in ADONIS offer greater flexibility and opportunity for the use of secure cryptoprinciples than do 26-point rotors. The United States has standardized on a family of developments, including teletype, utilizing 36-point rotors. The U.S. Joint Chiefs of Staff desire, therefore, not to project into the future a crypto-equipment for Combined and NATO use which would be incompatible with the rest of the United States cryptodevelopments. In view of the fact that the United Kingdom is compelled to use a single machine to meet both Commonwealth and Combined requirements, it seems that it would be to its immediate advantage also to standardize on a machine capable of using 36-point rotors.

b. The United States Joint Chiefs of Staff consider that gradual introduction of ADONIS beginning on 1 January 1955 is a practicable program which minimizes the possibility that adoption of ADONIS would result in further delay in replacing the CCM until the total requirement for ADONIS equipments can have been produced and distributed. This is supported by the status of production lines for mass production of an equipment capable of operating ADONIS.

c. Analyses which have been made on the best data obtainable as to the total cost of purchasing for U.S., Commonwealth, and NATO requirements for equipments, parts, and rotors for ADONIS as compared with the same for BRUTUS show that ADONIS is not only slightly cheaper from the standpoint of initial cost but also is considerably less expensive from the long-term standpoint. With the adoption of ADONIS many thousands of 10-15 year old, badly worn equipments which are slow and costly to maintain will be replaced by new equipments, whereas with BRUTUS many of these old equipments will have to be kept in operation through the use of adaptors. In order to enable the U.K. to meet the 1 January 1955

Enclosure

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
 Copy 24 of 35 copies  
 Page 4 of 6 pages

~~TOP SECRET - SECURITY INFORMATION~~

date for the initiation of the program, the U.S. <sup>would be</sup> is prepared to make available to the U.K., under arrangements to be determined later, U.S. ADONIS equipments, at least until the U.K. <sup>could</sup> can provide for its own version of ADONIS. I

d. Logistically, ADONIS offers many advantages.

(1) ADONIS makes it possible for a single machine, without adaptors (baskets), to be used by all countries in offices, vehicles, aircraft, submarines, and small vessels. Obviously, this means that standardization of operating and maintenance procedures, publications, keying materials, power supplies, and spare parts would be fairly simple. Although the same is technically possible with BRUTUS, it is not possible within the time proposed (January 1955).

(2) It offers the possibility for one type of rotor to be used throughout U.S./U.K. National, Combined, and NATO Commands. Also, as previously stated, the 36-point rotor used in ADONIS is used in certain U.S. teletype security developments which are under study by U.K. cryptographic experts for possible Combined usage. Extensive development engineering would be needed before the same could be true of BRUTUS.

(3) The power requirements, weight, and size of the version of ADONIS now in production makes it an acceptable cryptomachine for the lowest as well as the highest of Command echelons.

(4) ADONIS makes it possible for the distribution and accounting problems to be reduced to the minimum because of a reduction in the number and types of different registered items (rotors, adaptors, equipments, publications, spare parts, and components).

(5) Performance of and production capabilities for ADONIS equipment have reached the point where rapid expansion of

9/1 {

Enclosure

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
Copy 24 of 35 copies  
Page 5 of 6 pages

~~TOP SECRET - SECURITY INFORMATION~~

production is warranted and feasible. BRUTUS equipments have not reached this stage and production <sup>-line</sup> models will not be available until January 1954. Mass production on a scale similar to that of AF SAM-7 will not be reached until July 1954.

4. Therefore, it is urged that you accept the proposals in paragraph 2 and that you inform us of your acceptance as quickly as possible.

Action has been taken to increase the rate of production from 400 to 600 machines per month and preparations are being made for a further increase to 800 machines per month by the end of 1953.

Enclosure

~~TOP SECRET~~ CONTROL NUMBER 52-1534  
Copy 24 of 35 copies  
Page 6 of 6 pages