BRIEFING SHEET FOR THE CHAIRMAN, JOINT CHIEFS OF STAFF

JOINT CHIEFS OF STAFF MEETING, 1030, FRIDAY

16 JANUARY 1953

AGENDA ITEM NUMBER 6

J.C.S. 2074/23

SUBJECT: REPLACEMENT OF THE COMBINED CIPHER MACHINE

BACKGROUND:

1. U.S. and U.K. cryptographers have for some time worked toward replacement of the current Combined Cipher Machine (CCM). The U.S., in 1950, proposed to the U.K. that a cryptographic system called BRUTUS be adopted as the replacement. The U.K. accepted BRUTUS and planned to incorporate it in their own national machine. At the time BRUTUS was originally described to U.K. cryptographers, a U.S. system which is now called ADONIS was also demonstrated but was not proposed as a replacement for the CCM.

2. Early in 1952 the U.K. Chiefs of Staff indicated that adoption of one of the two U.S. machines nearing production (one incorporating the ADONIS system and another incorporating BRUTUS) appeared to be the only satisfactory and speedy solution to replacement of the CCM, and requested that U.S. machines be provided to the U.K. and the North Atlantic Treaty Organization (NATO) on a free loan basis. The U.K. Chiefs of Staff were informed that one of the two (ADONIS) would be ready for service tests by them beginning in mid-1952 and that if the tests proved the system satisfactory, a decision could then be made as to the ultimate CCM replacement. Later the U.K. Chiefs of Staff were informed that difficulties in production would delay the tests by six months.

3. The U.K. Chiefs of Staff now state (Enclosure "A" to J.C.S. 2074/21) that they desire a decision by 1 January 1953 as to which cryptographic principle will be adopted for Combined communications and recommend that it be BRUTUS, as originally agreed.

CURRENT REPORT:

4. This report is a revision of J.C.S. 2074/22 which was considered at the Joint Chiefs of Staff meeting of 5 Jan 53. It incorporates the instructions given at that meeting.

5. The reply informs the U.K. Joint Chiefs of Staff that the U.S. Joint Chiefs of Staff cannot concur in the recommendation for BRUTUS because the BRUTUS cryptoprinciple is no longer favored. It states that inasmuch as the ADONIS cryptoprinciple represents an important advance in security techniques and the 36-pt. rotors used in ADONIS offer significant flexibility and opportunity for using secure cryptoprinciples the U.S. Joint Chiefs of Staff are inclined most favorably towards ADONIS. The reply informs that the AFSAM 7, which embodies the ADONIS cryptoprinciple and is in production, will be service tested by the U.S. Services within the next 120 days and, if successful, will be adopted as a basic system for U.S. Joint communications.

6. The report emphasizes that the U.S. Chiefs of Staff recognize the potential dangers of the situation, with respect to inadequate amounts of equipment being available to U.K. Services for Combined and NATO communications, and acted to relieve it by making the ECM available to the U.K. To alleviate the urgency further and to enable the U.K. to initiate replacement of the present CCM by 1 Jan 55, the U.S. is prepared to make U.S. ADONIS equipments available to the U.K. until such time as the U.K. could provide its own version of ADONIS.

7. The reply concludes with the proposal that the decision as to the cryptoprinciple to be used in the new Combined Cipher Machine be deferred for 120 days until the results of service tests of the AFSAM 7 are known.

RECOMMENDATION:

8. It is recommended that J.C.S. 2074/23 be approved.

RALPH J. CANINE
Major General, US Army
Director, National Security Agency

Briefing Sheet prepared by Mr. Thomas R. Chittenden
Office of Communication Security
NSA, Ext. 60382

TOP SECRET CONTROL NUMBER 53-133
Copy 11 of 17 copies
Page 1 of 1 pages

cc: Secy, Joint Chiefs of Staff
ATTN: Mr. Kearney
NSA Pent. Liaison Group

V/DIR P/P (2) AG
C/S LOG
DDS R/D