CCM

3

BRIEFING SHEET FOR THE CHAIRMAN, JOINT CHIEFS OF STAFF

JOINT CHIEFS OF STAFF MEETING, 0915, WEDNESDAY

28 MAY 1952

AGENDA ITEM NUMBER 3

J.C.S. 2074/14

SUBJECT: SECURITY OF THE COMBINED CIPHER MACHINE

BACKGROUND:

1. The cryptographic security of the Combined Cipher Machine (CCM) has been of considerable concern to U.S. and U.K. cryptanalysts for some time, and several measures to improve its security have been taken, including replacement by a new cryptographic principle. A replacement target date of 1 January 1955, or sooner, has been agreed.

2. The U.K. Chiefs of Staff have proposed (Enclosure to J.C.S. 2074/11) that the ultimate replacement of the CCM be accomplished by the provision, by the U.S., of the cipher machines AFSAM 7 or AFSAM 47 to the British Commonwealth and NATO nations on a free loan basis. They state that the 7-rotor principle, which was accepted as a replacement for the CCM, in the form of an adaptor, for their TYPEX machine will not be ready before 1 January 1955, and that no suitable new British machine is sufficiently advanced in development to permit production within the next four years. The U.K. Chiefs of Staff point out further that the 7-rotor adaptor they have under development will be suitable for use only with the TYPEX, which does not exist in sufficient quantities to meet their share of equipments which will be necessary for NATO communications. The CCM's now used by NATO are provided in approximately equal quantities by the U.S. and the U.K.

CURRENT REPORT:

3. The draft memorandum to the British Chiefs of Staff informs them of the dates on which the requested equipments can be made available for service tests in the U.K., but asks for additional information on requirements of Commonwealth Nations before answering the request that the equipment be provided in quantity on a free loan basis. A plan of action is proposed to the British Chiefs of Staff for further consideration of this matter because it will depend, in part, on the outcome of the service tests which both the U.S. and the U.K. will conduct. Upon completion of security studies and service tests, the U.S. will recommend to the U.K. the equipment or equipments to be used for Combined and NATO communications, thus avoiding the likelihood that final choice of U.S. equipments would be governed too greatly by any selection the U.K. might make after service testing the two equipments. The reply proposes then that the economic and time factors involved be explored from the viewpoint of either complete replacement by new machines or whether partial use can be made of adaptors to present equipments.

4. It is further suggested to the British Chiefs of Staff that they consider the feasibility of producing in the U.K. either of the two equipments, both of which have been examined by U.K. engineers from a production viewpoint.

RECOMMENDATION:

5. It is recommended that J.C.S. 2074/14 be approved.

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

Briefing Sheet prepared by Mr. James H. Douglas
Ext. 60421
Plans and Policy Division

CC: General Bradley	(3)	Deputy Director, Army	(1)	Off. of R&D	(1)
Director, Joint Staff	(2)	Deputy Director, Navy	(1)	Off. of COMSEC	(1)
		Deputy Director, Air Force	(1)	Adjutant General	(3)
		Consultant	(1)	Plans & Policy Div.	(2)