~~SECRET~~ ~~SECRET - SECURITY INFORMATION~~

Suspense ~~15 Dec~~ 21 Jan

BRIEFING SHEET FOR THE CHAIRMAN, JOINT CHIEFS OF STAFF

JOINT CHIEFS OF STAFF MEETING, 1000, FRIDAY

7 NOVEMBER 1952

AGENDA ITEM NUMBER 2

J.C.S. 927/142

SUBJECT: RELEASE OF THE PRINCIPLES OF THE ECM TO THE U.K., CANADA, AUSTRALIA, AND NEW ZEALAND

BACKGROUND:

1. For Combined communications among U.S., U.K., Canadian, Australian, and New Zealand forces the Combined Cipher Machine (CCM) has been employed. It is also used in the North Atlantic Treaty Organization (NATO). Although the security of this machine has been improved in the past year by various means, cryptanalysts in both the U.S. and U.K. consider that the CCM does not afford as much security as is needed. Furthermore, there are not sufficient numbers of the CCM to meet all demands. New machines are being developed, however, to replace the CCM.

2. The ECM (Electric Cipher Machine), since its invention and development in the U.S. before World War II, has been reserved for exclusive U.S. use on the assumption that the cryptographic principle of the ECM was known only in the U.S. It has been known for several years that the U.K. does know the ECM principle and merely lacks knowledge of certain of its details which in themselves are not unique features of the cryptographic principle of the ECM. The U.K. has, in fact, developed for Commonwealth use and for offer to NATO, a teletype encryption machine whose cryptographic principles are very similar to the ECM, and adjudged to be more secure.

CURRENT REPORT:

3. The Armed Forces Security Agency Council has reconsidered the requirements for improving the security of Combined communications with the U.K., Canada, Australia, and New Zealand and has concluded that issue of the ECM, within the limits of availability, should be authorized.

4. The ECM, although containing the same basic cryptographic principle as the CSP 2900, differs in detail to the extent that loss of the ECM would not permit successful cryptanalytic attack on the CSP 2900. The CSP 2900 has not been disclosed to any foreign nation. The ECM is not in use currently by U.S. forces.

5. Release of the ECM will alleviate communication security problems due to shortage of CCMs, afford greater cryptographic security in selected high-level Combined communications, and will not endanger the cryptographic security of the U.S.

RECOMMENDATION:

6. It is recommended that J.C.S. 927/142 be approved.

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

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

CC: Secy, Joint Chiefs of Staff
ATTN: Mr. Kearney (5)
AFSA Pent. Liaison Group (2)

C/S
DDI
DDS
CONS
AG (2)
P/P (2)
R/D
C/SEC

~~SECURITY INFORMATION~~

~~SECRET~~