

~~TOP SECRET - SECURITY INFORMATION~~

BRIEFING SHEET FOR THE CHAIRMAN, JOINT CHIEFS OF STAFF

JOINT CHIEFS OF STAFF MEETING, 1400, MONDAY

5 JANUARY 1953

AGENDA ITEM NUMBER 2

J.C.S. 2074/22

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. The U.K. Chiefs of Staff are informed that for logistical reasons the U.S. Joint Chiefs of Staff cannot concur in the recommendation for BRUTUS and propose instead that:

a. ADONIS cryptoprinciple be designated as the new Combined and NATO cipher system.

b. The U.K. and U.S. jointly prepare a plan for the phased introduction of ADONIS to begin 1 January 1955.

c. The U.S. make ADONIS equipments available to the U.K. until the U.K. can provide its own version of ADONIS.

5. The reply to the U.K. Chiefs of Staff also gives detailed reasons for U.S. selection of ADONIS as the replacement for the CCM.

RECOMMENDATION:

6. It is recommended that J.C.S. 2074/22 be approved.


RALPH J. CANINE

Major General, US Army
Director, National Security Agency

Briefing Sheet prepared by Mr. Frank C. Austin
Communication Security Division
NSA, Ext. 60489

cc: Secretary, Joint Chiefs of Staff
ATTN: Mr. Kearney (5)
NSA Pent. Liaison Group (2)

V/SIR
C/S
JDS
CONS
AG
R/P (2)
LOG
R/D
C/SEC

Declassified and approved for release by NSA on 01-28-2014 pursuant to E.O. 13526

~~TOP SECRET CONTROL NUMBER~~ 53-3
Copy 11 of 17 copies
Page 1 of 1 pages