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. 2074/7
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 January 1951, to use this cryptoprinciple (Enclosure "B" to J.C.S. 2074/7).

2. The reply to the U,K. Chiefs of Staff contained in the enclosure states that although the problem is urgent, this urgency has been lessened by the U.S. action in releasing the ECM to the U.K. and is not now sufficient to warrant immediate adoption of BRUTUS. The reply states that the U.S. now favors the ADONIS cryptoprinciple. It recommends that the decision on the cryptoprinciple to be used in the new Combined Cipher Machine be deferred for at least 120 days pending the outcome of service tests of the AFSAM 7. Emphasis is placed in the reply on the fact that ADONIS offers considerable advances in crypto-techniques, flexibility of usage, and consistency with U.S. Joint planning.

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).

TOP SECRET

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 - SECURITY INFORMATION~~

ENCLOSURE

DRAFT

MEMORANDUM FOR THE REPRESENTATIVES OF THE UNITED KINGDOM CHIEFS OF STAFF

Subject: Replacement of the Combined Cipher Machine

1. The U.S. Joint Chiefs of Staff have studied the memorandum from the U.K. Chiefs of Staff, ACT 96, dated 5 December 1952, and regret that they cannot agree [redacted] to the proposals in paragraph 6 thereof.

2. The U.S. Joint Chiefs of Staff agree as to the urgency of reaching a practicable and acceptable solution to the problem but do not believe that the urgency is such as to compel immediate adoption of BRUTUS, which embodies a cryptoprinciple they no longer favor.

3. The U.S. Joint Chiefs of Staff are now inclined most favorably toward the adoption of the ADONIS cryptoprinciple, which represents important advances in crypto-techniques. They consider that the 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 cryptoprinciple for Combined and NATO use which would be incompatible with other United States cryptodevelopments. In view of the fact that the United Kingdom is compelled to use a single machine to meet U.K., Commonwealth, Combined, and NATO requirements, it seems that it would be to the advantage of the U.K. also to standardize on a machine capable of using 36-point rotors.

4. The U.S. Services have already agreed that the ADONIS crypto-principle will be adopted at an early date as a basic system for U.S. Joint communications, if service tests (field trials) prove the AFSAM-7 satisfactory.

5. Although the U.S. has experienced [redacted] delays in the production of its embodiments of the ADONIS cryptoprinciple, one of these embodiments, the AFSAM-7, is now well in production and service tests by U.S. Services

of final production models will be completed within the next 120 days. The U.S. has already supplied the U.K. with one of the recently delivered pre-production models of the equipment, for study and familiarization, and plans to furnish 10 to 15 final production models (previously scheduled for delivery by 1 January 1953) by 1 March 1953, for U.K. field trials.

6. If upon completion of the U.S. service tests of the AFSAM-7, the U.S. Joint Chiefs of Staff determine that the equipment has proved to be acceptable, they will recommend the adoption of the ADONIS cryptoprinciple for Combined and NATO use.

7. The U.S. Joint Chiefs of Staff appreciate the apprehensions of the British Chiefs of Staff that outbreak of hostilities might find the British Services inadequately equipped for secure National, Combined, or NATO communications. They have therefore explored the possibility of allaying these apprehensions.

a. In January, 1950, the U.S. Joint Chiefs of Staff assured the British Chiefs of Staff thay they would endeavor, in the event of an emergency occurring before the new CCM became available, to provide the U.K. with a limited number of cipher machines of adequate security to meet immediate urgent needs of highest command Combined communications. Rather than wait for an emergency the U.S. Chiefs of Staff have authorized the Director of the National Security Agency to disclose the ECM principles to appropriate U.K. authorities and with them to plan for the introduction of available quantities of ECM's for Combined communications. It is understood that as a result of recent planning in the U.K. and the U.S., involving Combined use of the ECM and redistribution of the CCM, a significant additional quantity of CCM's is now available. This action together with a recent revision downward of NATO requirements for the CCM indicates that the latter can now be substantially met.

b. In order to enable the U.K. to meet the 1 January 1955 date for the initiation of the program for the replacement of the Combined Cipher Machine, the U.S. would be prepared to make available to the U.K.,

TOP SECRET

~~TOP SECRET~~

under arrangements to be determined later, U.S. ADONIS equipments, at least until the U.K. could provide for its own version of ADONIS.

8. The U.S. Joint Chiefs of Staff, therefore, ~~recommend~~ propose that the decision as to which cryptoprinciple be adopted in a machine to replace the present Combined Cipher Machine be deferred for 120 days, until the results of the service tests of the AFSAM-7 have become known.

b. If the AFSAM-7 proves to be satisfactory, the U.S. Joint Chiefs of Staff will propose to the U.K. ~~U.K. and the U.S. Army~~ that the cryptoprinciple of BRUTUS to adopt the ADONIS cryptoprinciple for Combined and NATO use and then prepare a plan for the phased introduction of ADONIS to begin on 1 January 1955.

TOP SECRET