INCL 2

~~TOP SECRET~~ 14 June 1950

PROPOSED DRAFT OF REPORT TO JCS - BASED ON ADMIRAL STOKES'S PAPER

Paragraphs 1 - 7, no change.

Rest of paper, cancel and substitute:

PROBLEM AND DISCUSSION (Continued)

8. The problem of security of combined communications is of much greater magnitude and complexity for the Navies concerned than for the respective Armies and Air Forces. For example, during World War II, the U.S. Navy procured and used 15 times as many SCM's as the U.S. Army and U.S. Air Force combined. Yet the CCS distribution was limited to "Major War Vessels" (destroyers and above). Other U.S. Naval requirements for which no satisfactory crypto-systems are available include the following categories of combined communications:

Submarines (Submarine Warfare)

Minor War Vessels (Anti-Submarine Warfare and Amphibious Operations)

Merchant Ship Control

These requirements must be met regardless of what type of cryptographic systems are adopted for the High-Command, Major War Vessels, or combined communications of other categories. The U.S. and British Navies strongly desire to have all combined communications (with the possible exception of High-Command Communications) conducted in the same basic cryptographic system and by means of the same cipher machine, using different sets of keying elements for

~~TOP SECRET~~

different categories of communications. Since 1944 the U.S. Navy has been developing a small "portable" cipher machine (the PCM) to fill the special requirements of Submarines and Minor War Vessels. The PCM will be cryptographically identical with the 7-rotor SCM, and equally suited for Merchant Vessels and Major War Vessels. Development of this machine should be completed by November 1950. Both the PCM and SCM have provision for communicating with the present CCM to provide for the transition from old to new systems. Regardless of what action is taken in the matter of replacing the present CCM for High Command and Major War Vessels, the U.S. Navy is going to have to adopt the PCM and SCM for its own essential wartime communications.

9. Examination of the drawings of the proposed new British crypto-machine indicates that minor alterations would be sufficient to adapt it to work with the 7-rotor SCM. However, since the new British machine is in the early stages of development and the new U.S. PCM machine is nearly completed, it would expedite production as well as reduce overall costs to the U.K. for the British to adopt the PCM for their own intra-service use as well as for combined use.

CONCLUSION

10. The U.S. policy of not sharing the SCM (either in the original SCM/-igaba, in the improved CSP's 2500 and 2900 forms, or in any modifications which may be made hereafter) should be adhered to by the U.S. Joint Chiefs of Staff.

DISCUSSION (cont'd)

11. Although it is possible to modify the present U.S. cipher machine to work with the proposed British cypher machine, such a course would be undesirable for reasons given above.

12. The Navy has paramount interest in the Combined Cipher Machine, the requirements of the Army and Air Force being negligible in comparison.

13. The interests of efficiency, economy, reliability, and meeting the target date would best be served by adopting the 7-rotor M[illegible]/FCE for the new combined cipher machine.

RECOMMENDATIONS

14. It is recommended that:

a. The proposition of directly adapting the M[illegible]/SIGABA to the proposed new British cypher machine be abandoned.

b. The 7-rotor M[illegible]/FCE be approved by the U.S. Joint Chiefs of Staff for all categories of combined communications, and submitted to the British Joint Chiefs of Staff.

c. The U.S. reply to MMC 1/46 dated 14 February 1946 (JCS 2074/3) be in substance as follows:

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE (CCM)

The U.S. Chiefs of Staff have examined the drawings of the proposed new British cypher machine, forwarded with MMC 1/46 dated 18 April 1946, and wish to make the following comments and proposals.

(a) Modification of present U.S. cipher machines to operate with the proposed new British cypher machine.

Although it is possible to modify present U.S. machines and the

~~TOP SECRET~~

REPLACEMENT OF THE PRESENT
"COMBINED CIPHER MACHINE" (CCM)

proposed new British machine to operate together; this ~~possibi-~~ Alternative
~~lity~~ is unsatisfactory and cannot be accepted by the U.S. Joint Chiefs of Staff.

(b) Adoption of new 7-rotor machines for future combined communications.

(1) The development of the 7-rotor [redacted] and its cryptographic equivalent, the small 7-rotor Portable Cipher Machine ([redacted]), have been carried to the point where the U.S. Joint Chiefs of Staff can approve them in principle for all levels and all categories of Combined Communications.

(2) The 7-rotor [redacted] has provision for communicating with the present 5-rotor CCM and is thus capable of interim use.

(3) The 7-rotor [redacted] is submitted for consideration as the new Combined Cipher Machine.

(4) If accepted for combined use, the U.S. is willing to furnish manufacturing drawings, engineering specifications and working models of the 7-rotor [redacted] and 7-rotor [redacted] to the U.K.