TOP SECRET

COPY

WAR DEPARTMENT SUMMARY SHEET

For 1 APPROVAL

WDGID

TO:

1 CHIEF OF STAFF

Lt. Col. Hiser/8129 Ext 462
24 Apr 1947

U.S. and British Collaboration on
Combined Cipher Machine Development

SUMMARY

1. Pursuant to verbal authority, discussions were held with representatives of the British Government on the matter of improving the security of the Combined Cipher Machine. The results of the conferences as agreed upon by British and U.S. representatives are as set forth in Tab A. Although a definite agreement was not reached, a firm basis therefor was established.

15

2. The following outlines the presentation made by the British representatives at the opening meeting:

a. In the opinion of the British, the present Combined Cipher Machine (CCM) is not sufficiently secure to resist increasingly effective cryptanalytic techniques. In addition, the British are anxious to develop a replacement for their present high level cipher machine (Typex).

b. For reasons of economy the British feel it desirable that any new intra-service machine developed by them be adaptable for Combined use and for this reason they are anxious to participate in parallel research and development with the U.S.

c. The British indicated that they were aware of the principles of the high grade U.S. cipher machine, SIGABA (ECM). They described this equipment quite accurately, considered its security to be of the highest order, and stated, in fact, that they had incorporated its principles in a radioteletype cipher machine for their own use.

d. The British stated that they had developed an idea which they termed as "new and revolutionary" which they feel is superior to the SIGABA principle. They further indicated

Incl 15

COPY

that if the U.S. were willing to consider the eventual replacement of the SIGABA with something more secure, they would like to make available their new principle for a cipher machine which could be used for Combined as well as intra-service communications. If, however, the U.S. did not contemplate replacement of the SIGABA, the disclosure of their new ideas would be only of academic interest. In the latter case, the British suggested that the SIGABA principle be incorporated in a new CCM, which principle they would also incorporate in their intra-service machine.

3. a. It has been U.S. policy to withhold the cryptographic principle of the SIGABA from all foreign powers, including the British. Therefore, in spite of obvious British knowledge of the principle of this device, discussions were temporarily discontinued in order that the U.S. policy could be reexamined in joint session.

b. At the joint conferences, the Army representatives took the position that they could see definite advantages and no serious disadvantages to the U.S. in the release of the SIGABA principle for incorporation in a new Combined Cipher Machine, and in view of the circumstances, were desirous of recommending to higher authority the reconsideration of the existing policy of non-disclosure of the SIGABA principle. However, in deference to serious objections on the part of the Navy representatives, it was finally jointly agreed to inform the British that the SIGABA principle could not be discussed. As a result, that phase of the matter was completely eliminated from discussion during subsequent Combined meetings.

4. Upon receipt of the decision indicated above, the British representatives made a complete disclosure of their "new and revolutionary" idea. The U.S. representatives were unable to accept it due to engineering and maintenance difficulties which, in their considered opinion, would make a device based thereon impractical. The British representatives, in spite of this adverse opinion, stated that they expect to continue development of equipment incorporating these principles and indicated that the results of their work would be made available to the U.S., if in their view it might have Combined application.

5. The U.S. representatives then presented their own ideas for the improvement of the security of the Combined Cipher Machine. These ideas will be studied by the British from the viewpoint of corroborating the U.S. estimate of enhanced security. At the same time, the U.S. will continue its research from the viewpoint of practical, or engineering and maintenance,

COPY

problems introduced by the proposed changes. These British and U.S. studies will require approximately three months and after study of the results by all concerned, it should be possible to reach a definite conclusion in a total of six months.

6. a. The British representatives indicated their desire to collaborate in the development of a cipher machine for Combined use in lower echelons; however, the U.S. representatives lacked authority to enter into such discussion. The British urged that the necessary authority be requested.

b. During the war just ended there was a need for such a device. As a result of practical experience the British are in a good poisition to contribute basically new and improved ideas to cryptographic projects, and it is therefore believed that collaboration would be useful and advantageous to the U.S.

7. As a preliminary to further collaboration, however, the U.S. representatives proposed that Combined Communication Security Regulations be established in order to standardize the protection afforded combined cryptographic material. This proposal was taken under advisement by the British, who will prepare a draft set of regulations. Both the British and the U.S. will submit their respective drafts to the Combined Communications board in order to obtain a mutually acceptable set of combined regulations.

RECOMMENDATION

It is recommended that contingent upon the establishment of a set of Combined Communication Security Regulations and subject to concurrence of the U.S. Navy, authority be granted to collaborate with the British: (a) In the improvement of the Combined Cipher Machine, and (b) In the development of a low echelon cipher machine for combined use.

Approved 2 May 1947 by order of the Secretary of War, THOS. T. HANDY, Deputy Chief of Staff, "subject to clearance with SWNCC and within present budgetary and manpower limitations."

/s/ Victor L. Cary
for W. E. Thurman
Lt. Col GSC Asst to the Deputy Chief of Staff

/s/ Walter E. Todd
WALTER E. TODD
Brigadier General, U.S.A.
Deputy Director of Intelligence