REPORT BY AD HOC COMMITTEE

to the

ARMED FORCES SECURITY AGENCY COUNCIL

on

REPORT OF THE UK/US COMMUNICATION SECURITY CONFERENCE, 1952

THE PROBLEM

1. To study the implications of paragraph 9d of "Report of the UK/US COMSEC Conference" (AFSAC 63/63) which recommended release of the British device "Mercury" to NATO.

2. To study the question of the release of the CSP 2900 to the British for purely Combined use, as an interim solution to the replacement of the CCM.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

3. See Enclosure "B".

CONCLUSIONS

4. It is concluded that:

a. Paragraph 9d of "Report of the UK/US COMSEC Conference" (AFSAC 63/63) should be approved. There should, however, be added to the report a general note to this effect:

> "In all cases where crypto-equipments are to be made available to NATO, the revelation of cryptoprinciples involved should be restricted to general summaries and descriptions, and should not include specific wiring details, drawings, etc., until after the equipment is in production."

b. The development by the UK of a cipher machine incorporating principles so similar to those of the CSP 2900 as are those of "Mercury" makes it obvious that the principles of CSP 2900 can no longer be regarded as the exclusive property of the US; but there

is still valid reason for continuing to keep from the UK detailed knowledge of the CSP 2900. There is not, however, any valid reason for continuing to keep from the UK detailed knowledge of the ECM.

c. There are uses, in Combined communications, to which the available quantity of ECMs might well be put, and these uses would improve the security of Combined communications.

RECOMMENDATIONS

4. It is recommended that:

a. The conclusions be approved.

b. The memorandum attached as enclosure be forwarded to the Joint Chiefs of Staff.

c. The "Report of the UK/US COMSEC Conference" be amended to include the paragraph contained in paragraph 4a of the Conclusions.

ENCLOSURE "A"

DRAFT

MEMORANDUM FOR THE JOINT CHIEFS OF STAFF

SUBJECT: Release of the Principles of the CSP 2900 to the U.K., Canada, Australia, and New Zealand

1. The cipher machine CSP 2900 and its predecessor, the ECM, have been retained for exclusive US use under the terms of paragraph 30813e of "Joint Action of the Armed Forces."

2. The Armed Forces Security Agency Council, having studied the requirements for improving the security of Combined communications with the United Kingdom, Canada, Australia, and New Zealand, now recommends that the principles of the ECM be authorized for release to the above-mentioned countries, and that issue to them of the ECM, within the limits of availability, also be authorized. These recommendations are based on the following reasoning:

a. The UK has developed, for Commonwealth use and for offer to the NATO nations, a teletypo cipher machine known as "Mercury" which has a cryptoprinciple very similar to that of the CSP 2900 and is adjudged by the US experts to be even more secure. The similarity in principle, even though the details differ and the CSP 2900 is not a teletype machine, makes it apparent that the basic principle of the CSP 2900 can no longer be considered exclusively US. There is no evidence, however, to indicate that the details of the CSP 2900 are known to anyone other than US personnel.

b. The ECM, although containing the same basic cryptoprinciple 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.

c. The CCM, in current use for Combined communications, is outmoded, exists in insufficient quantity to meet all demands, and, particularly from the standpoint of high command communications and those dealing with intelligence, is considered inadequate.

d. The US Armed Forces are now operating under an agreed "Plan for the Development and Use of Cryptographic Equipment and Principles." The long-range portion of the plan provides for the development of equipments which will be retained for exclusive US use in both the literal and the teletype communications security fields.

e. In the meantime the US, although releasing the details of the ECM, would continue to retain inviolate the details of the CSP 2900. Retention of these details for exclusive US use satisfied the requirement of paragraph 30813e of "Joint Action of the Armed Forces."

3. It is recommended that the Joint Chiefs of Staff approve:

a. Disclosure of the details of the ECM to appropriate British authorities (Cypher Policy Board) by the Director, Armed Forces Security Agency.

b. Initiation of action by the Director, Armed Forces Security Agency, with appropriate British authorities (Cypher Policy Board) for utilization in Combined communications of such ECMs as can be made available.

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. With regard to part 1 of the problem:

a. "Mercury", a British-invented device, contains cryptoprinciples so similar to those of the CSP 2900 that to offer the former to NATO amounts to giving away those principles which the US has retained for its own use in the past.

b. Loss to an enemy of the "Mercury" would in no way endanger the security of US communications enciphered in the CSP 2900, since, although similar in principle, Mercury and the CSP 2900 differ in detail.

c. Complete revelation to other NATO nations of the minute details of any cryptoprinciple prior to its embodiment in a manufactured version is a practise to be avoided, since such detail would permit a nation to produce its own embodiments even though the final US equipment might be officially rejected for NATO use.

2. With regard to part 2 of the problem:

a. The CCM currently in use for Combined as well as NATO traffic is outmoded and inadequate, particularly for highest-level and intelligence traffic.

b. The appearance of the principles of the CSP 2900 in "Mercury" makes it obvious that the cryptographers of the UK are thoroughly familiar with the broad principles of the CSP 2900. This does not mean, however, that the UK is familiar with the details of application of the principles within the CSP 2900.

c. The CSP 2900 includes the same basic principles as does the ECM, its predecessor, but again differs sufficiently in detail to mean that revelation of the principles of the ECM would not provide exact knowledge of the CSP 2900. Cryptanalytic attack with high speed analogues requires knowledge of specific details; therefore, even should knowledge of the details of the ECM become known to an enemy cryptanalyst, he could not

use that knowledge to direct intelligently a high speed analogue attack on the CSP 2900.

d. Release of the ECM to the UK would permit use of a very strong machine for some Combined communications and would still permit compliance with paragraph 30813e of Joint Action of the Armed Forces, which requires retention for exclusive US use of our most secure cryptographic system. Such release would not jeopardize the security of US communications.

e. There are not sufficient quantities of either CSP 2900 or ECM in existence to permit the offer of any large quantity to the UK. They are sufficient, however, to meet some of the more urgent high command and special requirements. The UK, if such an offer were to be made, should have a voice in determining the uses to which the quantity which could be offered might best be put.