~~TOP SECRET SECURITY INFORMATION~~ 30 June 1952

REPORT TO THE CHAIRMAN, ARMED FORCES SECURITY AGENCY COUNCIL

Special Report of AFSAC Ad Hoc Committee on Release of CSP 2900

1. In accordance with instructions issued by the Chairman, AFSAC at the meeting of 20 June 1952 an Ad Hoc Committee met on 24 June 1952 to study:

a. The implications of paragraph 9d of the Report of the UK/US COMSEC Conference (AFSAC 63/63) which recommended the release of Circuit Mercury to NATO.

b. The question of the release of the CSP 2900 to the UK for purely Combined use, as an interim solution to the replacement of the CCM.

Members present were:

Colonel R. C. Sears, AFSA, Chairman

Colonel J. L. Weeks, AFSS

CDR R. L. Taylor, USN

Mr. A. W. Small, ASA

Others present were:

Major E. J. Giese, USAF

Major D. T. Woodruff, USAF

CDR F. A. Raven, USNR

Major O. A. Davis, SigC

Mr. D. Wolfand, ASA

LtCol H. B. Blacksten, AFSA

Dr. R. H. Shaw, AFSA

Mr. C. W. Wernle, AFSA

2. The Ad Hoc Committee considered the implications of releasing Circuit Mercury to NATO. It was observed that Mercury contains crypto-principles so similar to those of the CSP 2900 that to offer the machine to NATO would mean giving away these principles which the US has steadfastly retained for its own use in the past. However it was agreed that these cryptoprinciples are no longer known only to the US and it would be nothing but a "head in the sand" attitude to continue to withhold them from our allies. It was also agreed that the possibility of loss of the equipment to an enemy would in no way further expose US BACCHUS communications to cryptanalytic attack. The committee therefore recommends approval of paragraph 9d of the report, subject to a comment stating that, "In all cases wherein crypto-equipments are to be made available to NATO, cryptoprinciples will not be divulged to NATO prior to actual production and distribution of the equipment".

3. The Ad Hoc Committee considered the question of the release of the CSP 2900 to the UK, for purely Combined use, as an interim solution to the replacement of the CCM. The Ad Hoc Committee agreed unanimously that not the CSP 2900 but the ECM/SIGABA (CSP 889) should be released to the UK for High Command Combined communications to the extent that the US Services can supply them. If replacement is to the full extent that High Command Combined systems are now established, the requirement will be approximately _____ ECM's. If distribution is limited to Class 7 holders the requirement will be approximately _____ machines. The following points were considered in arriving at this recommendation:

a. The CCM is completely outmoded and inadequate, particularly for the encipherment of Combined High Command traffic. An immediate replacement by a more adequate machine is highly desirable.

b. The cryptoprinciples employed in CSP 2900/ECM are well known to UK cryptographers.

c. The US must be protected against the ability of an enemy, having constructed a high-speed analogue for solving a UK/US machine, to use this analogue to read US BACCHUS communications. For this reason it is not desirable to provide the CSP 2900 in its present form to the UK.

d. A wiring change to the CSP 2900 would be sufficient to protect US BACCHUS against the possibility mentioned in (c) above, but this would require modification of existing CSP 2900 machines and would require US holders to hold two different machines.

e. The same degree of protection can be achieved by providing the UK with the ECM/SIGABA. There are approximately 2000 of these machines in existence in the US Services in a non-operational reserve status. Also since CSP 2900 has a switch which permits intercommunicability with ECM/SIGABA this precludes the necessity for US holders to hold two different machines.

f. The number of CSP 2900's available to the US will be reduced by the number of ECM/SIGABA made available in accordance with the above, due to the conversion program. But in any arrangement to provide CSP 2900 type machines some reduction in availability

will result. The provision of ECM/SIGABA will involve a minimum of such reduction due to considerations set forth in subpara. (d) above.

4. It is recommended that the conclusions contained herein be approved and the matter be referred to AFSA for the preparation of the necessary JCS implementing directives.

R C Sears

R. C. SEARS
Colonel, USAF
Chairman, AFSAC
Ad Hoc Committee