SECRET

14 July 1952

MEMORANDUM FOR MR. FRIEDMAN

    1. At your request, I have prepared this memorandum setting forth my views on the ad hoc committee report on release of CSP 2900.

    2. I cannot, of course, quarrel with the idea of release of the ECM to the British, since I have been in favor of such release for about seven years. I do believe, however, that the offer comes much too late to be of any value, and my opinion is that the British are likely to reject the offer unless at least one of the following is true:

        a. The release will be extended to NATO and will include CSP 1600 (Sigamug) adapters.

        b. The number of machines available for loan is enough to outfit completely the UK Navy, and there are also enough CSP 1600 adapters. This would then release many CCMs for NATO use.

        c. There are some very limited special requirements which might be taken care of by a limited number of machines.

    3. With regard to 2.a, and also to 2.b, the British have expressed to me several times that they believe the day of UK/US communications to be coming to an end. Their opinion, which I share, is that NATO traffic is now of paramount importance. There is an ever decreasing amount of traffic now which is confined to UK/US channels. There will always be some, of course, but the UK, the US, and Canada are no longer a triumvirate entire unto themselves, but are rather the leaders in a larger alliance, NATO, and nearly all of their important traffic (outside of Korea) deals with the affairs of that larger alliance. NATO, too, is where we are hurting the most, as far as cipher machines are concerned, and this release of ECM to the UK does not help NATO. There are several ways in which ECM distribution to NATO or to the British could be worked out, but I know of none that would be satisfactory on less than about 1200 machines.

    4. In addition to not easing the NATO difficulty, limited distribution of ECM to the UK forces them into the always annoying requirement of holding two different machines. They don't like this, especially Navy-wise, even at the high levels. However, there are perhaps some requirements which might be eased by issue of ECM in limited quantities and might make the matter worth pursuing. I am thinking of the COMINT communications problem and particularly SSO and BLO traffic (on which I have another memo on the way to you).

1

SECRET
SECRET

5. I have these specific comments on the report of the ad hoc committee:

a. As a report, it does not provide a basis for decision on the question of furnishing any real help, since it does not say how many machines will be available. The implication is that it will be a small number, but the report doesn't say, even though it obviously is not intended to be anything as broad as 1200 machines. I have heard that the figure/50 was the one that seemed most sensible to the committee. Furthermore, the report does not consider the requirements for additional CSP 2900s for US use, which the US Services have stated to be so large as to require that completely new equipments be manufactured. (Nevertheless, when approaching the British we must be able to give them a definite figure.)

b. The report calls this release an "interim solution to the replacement of the CCM." It obviously is not, unless it's to be on a very wide scale.

c. Although paragraph 3.c is correct, it is misleading and should be changed to read:

"Assuming that an enemy might have the ability to construct a high-speed analogue for solving a UK/US machine, the US must be protected against the possibility of his extending use of this analogue to the reading of US BACCHUS communications. For this reason, it is not desirable to provide the CSP 2900 in its present form to the UK."

d. The comment to be added to AFSAC 63/63 as quoted in the last sentence of paragraph 2 of the report is totally unrealistic and virtually impossible of compliance. Cryptomaterial is not only released or made available to NATO; it must also be accepted by NATO. It is impossible to get NATO approval of a crypto-equipment, particularly the new crypto-equipments, without releasing the cryptoprinciple for study and acceptance, and if we wait until the equipment is produced and distributed before releasing the principle, we create delays of months, perhaps even years, in supplying NATO. I think I know the intent of this comment, and I believe it should read:

"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."

2

SECRET

~~SECRET~~

6. To summarize, I have the following recommendations to make:

a. Find out how many equipments will be offered by each Service and when.

b. If the number is about 1200, broaden this report to include release to NATO.

c. If this is totally unpalatable, proceed with the idea of issue to the UK navies, and prepare specific proposals to be sent to the British.

d. If the number is no where near 1200, rewrite the paper to include specific ideas as to how to best make use of the limited quantity, then make specific proposals to be sent to the British.

e. In any event, re-do the paper to ~~inderperate~~ reflect my comments in paragraph 5.

FRANK C. AUSTIN
Chief, Analysis and
Evaluation Division

~~SECRET~~