INTRODUCTION

We remain convinced of the urgent need for an effective approach to the French and, after study of the set of papers covered by your MOP.5509 of 23rd December, we are prepared to accept the new basis of approach subject to the modifications and amendments described below. These in our view have the effect of bringing it more into line with the June Agreements but retain the emphasis on the preparation of a memorandum for the Standing Group as the starting point for the technical discussions.

GENERAL MODIFICATIONS

2. We consider that the tabling of a Minimum Standards Paper, particularly in its present form, is likely to hinder rather than help the implementation of paragraph 18B of the June Conference Report. We accordingly propose that the original purpose of the Minimum Standards Paper should be adhered to, viz: "Providing guidance to SECAN and EUSEC and for establishing a basis for giving advice to each country".

3. The main objections to handing such a paper to the French are the same as those we made in June to publication to NATO nations of the Minimum Standards Paper:-

(a) It is unlikely to induce discussion of how particular cyphers may be improved.

(b) Any such paper must necessarily be comprehensive and therefore contain matter irrelevant to the problems of any one nation.

The purpose of initiating the required type of discussion with the French will, we are convinced, be better served by the "brief for Delegates to the Technical Discussions" as amended in the appended documents.

4. There are many technical points in the "Minimum Standards" paper with which we disagree. We therefore propose that we should forward CCHR and Cirsch Agency comments to NSA and that final agreement should be reached on all points relevant to the discussions with the French at the preliminary meeting of the U.S. and U.K. delegates in London.
1. Agreed Portion of Brief for approach to the
French on Communications Security by U.S.
and U.K. Ambassadors.

2. Aide Memoire.

3. Agenda and Brief for the Meeting of Delegates
from Turkey.

4. Brief for Delegates to Technical Discussions

---

(a) Substitute for para 2 the following new para 2-
"It is therefore necessary to take steps to ensure that no
NATO country uses, for its national communications, inadequately
secure cryptographic and transmission practices which could
disclose significant information to a potential enemy*.

(b) Substitute for para 5 the following new para 5-
"The Governments of the U.S. and U.K. propose, therefore, that
technical discussions among the Communications Security
experts of the three standing group powers be held forthwith
with the object of agreeing upon a memorandum for issue by the
Standing Group to all NATO Governments. The U.S. and U.K.
Governments are, however, conscious of a number of weaknesses
in their own national communication practices; the French
Government may also have noted similar weaknesses in its own
practices. The U.S. and U.K. Governments believe that it is
essential for the U.S., France and the U.K. to assure themselves
that their own standards of Communications Security are of a
level mutually agreed to be satisfactory and further propose
that action adequate to this end be initiated during the
above technical discussions and before the issue of the
memorandum by the Standing Group."

---

(a) Para 2, sub-para (d): Delete final sentence and add to
penultimate sentence:
"...and in discussion of its appendix: List of Dangerous
Practices. The U.S. and U.K. delegates will try to reach
agreement with the French on systems that are fundamentally
insecure and practices that must be forbidden and seek to get
the List of Dangerous Practices accepted, or preferably
amplified."
4. Brief for Delegates to Technical Discussions (contd.)

Delete sub-paras (a) through (h) and substitute new sub-para (e) as follows:

"Every effort must be made to induce the French to discuss their own ciphers, communications practices and procedures. In moving from the above theoretical discussions to practical issues delegates may hope to elicit from the French something of what they already know by referring to SECAN's and our own experience in COMSEC. The exact tactics will be agreed between the U.S. and U.K. delegates, initially at the preliminary talks in London and, subsequently, as may be necessary, by private consultation in the light of the course the discussions take. Such tactical decisions will be governed by the provisions of sub-para (c) above."

(b) In para 3 a(2) insert after U.S. "...and U.K.".

(c) Substitute for sub-para 4(b), new sub-para 4(b) as follows:

"COMSEC = If the French ask, pointblank, questions about national cipher systems of the U.S. or U.K. a frank answer should, wherever possible, be given. If the reply to such a question would involve revelation of principles not approved by the U.S. and U.K. for release, attempts should be made to evade the question discreetly. In the last resort the reply should be that this particular subject is one which the delegation is at present unable to discuss."

5. Standing Group Memorandum.

No change.


Proposed detailed amendments by bag.
3. Limits of Cryptographic Access.

(a) The disclosure of U.S. or U.K. cryptographic secrets shall be limited to:

(1) The systems that are used by U.S. or have been officially proposed for U.S. use;

(2) The systems and equipment that by the time of the conference may have been approved for release to the French as a result of their request for assistance for their foreign office.

(3) The U.K. method of making one-time pads by Bletchley, with the procedures and standards of checking.

(4) The U.S. method of making one-time tapes by DONALD DEE (with a statement that U.S. methods are similar) and the procedures and standards used for checking.

4. Predictable Sources of Discontent.

(b) CORDON - It is possible that the French might ask, point-blank, "what are the principles of the cipher system used by the U.S. Dept. of State, or by the U.S. Army at high levels, or by the British Navy?" If such a question should arise, the answer should simply be that each country (U.S. and U.K.) has a national security policy which prohibits revelation of such information except as explicitly approved. This should be a satisfactory reply, since the list of approved systems is already quite restrictive, and since the French themselves will not have been asked similar questions. For any system used by the French there is either a good reason for the U.S. and U.K. to keep its details and the fact of its use, or the system is so generally known to cryptography as to make CORDON judgment an obvious error.
The following device may be used if at any stage it appears to both the U.K. and U.S. delegates that it will further the real purpose of the discussions. The U.S. Delegation will have been provided with a suitable version of the "Minimum Standards Paper", the final text of which shall have been agreed during the preliminary discussions in London. At some natural point, for instance when the French Delegation have queried the reason for some restriction proposed by the U.K. and the U.S., or when some basis is required for a statement in the "List of Dangerous Practices", the U.S. will make available to the other delegates either the whole of this document or relevant sections, as if it were one of the U.S. reference papers which they feel the others might just as well see and which would in all probability represent a brief, or part of a brief, for the guidance of SECAN. In arranging the procedure for the introduction of this paper the U.K. and U.S. delegates will bear in mind that it must not take on the appearance of a document jointly prepared and that it is not to be presented as an official action paper. If the whole document is made available it must be ensured that the French understand that SECAN would not propose to issue such a paper and that it must not be discussed outside those tripartite discussions.