U.K. COMMENTS ON THE U.S. DRAFTS FORWARDED TO LONDON, DECEMBER 23rd, 1953.

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.3609 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 GCHQ and COMSEC 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.

G.C.H.Q. COMMENTS ON U.S. DOCUMENTS ON FRENCH COMMUNICATIONS SECURITY.

1. Agreed Portion of Brief for approach to the French on Communications Security by U.S. and U.K. Ambassadors.	:	No Change.
2. Aide Memoire.	:	(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.K. and U.S. 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.K. and U.S. 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."
3. Agenda and Brief for the Meeting of Delegates from T.S.W.G.	:	No Change.
4. Brief for Delegates to Technical Discussions	:	(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 (e) through (h) and substitute new sub-para (e) as follows :-

"Every effort must be made to induce the French to discuss their own cyphers, communications practices and procedures. In moving from the above theoretical discussion to practical issues delegates may hope to elicit from the French something of what they already know by referring to SECAM'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 1(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 cypher 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.

6. Communications Security Principles and Minimum Standards. : Proposed detailed amendments by bag.

AIDE - MEMOIRE.

U.S. VERSION.

1. The U.S. and U.K. Governments have reached the conclusion that the national communications practices of many NATO governments may be such as to create a potential source of highly valuable information to the USSR. The U.S. and U.K. Governments also are of the opinion that the French Government may have reached a somewhat similar conclusion independently. The U.S. and U.K. Governments believe that the security of NATO as a whole depends on the security of each individual member government and, consequently, that it is in the common interest to take action immediately to bring this situation to the attention of all NATO governments.

2. The problem is whether -- with respect to what constitutes adequate cryptographic or transmission security -- the currently accepted standards of any of the NATO nations are less than satisfactory.

3. It is the view of the U.S. and U.K. Governments that the problem of the communications security practices of the NATO governments should be handled through the Standing Group in somewhat the same manner as - and as an extension to - the previous activities of this Group in establishing the communications security practices of NATO. It is realized that the Standing Group was created to issue directives only on the military affairs of NATO. It is known, however, that some NATO governments currently desire advice on their communications security problems; the Governments of Belgium and Italy already have written to the Standing Group on the subject. It seems proper, therefore, to use the Standing Group, which is conveniently available, in an advisory capacity on a matter which ultimately does relate to the security of NATO.

4. The U.S. and U.K. Governments together believe that the U.S., France and the U.K. should join in preparing a memorandum for the Standing Group to issue to all member governments and that this memorandum should :-

(a) Re-emphasize that the security of NATO as a whole depends upon the security of each individual nation and that, consequently, secure national communications practices form a vital part of NATO security.

(b) Contain a preliminary list of examples of dangerous cryptographic and transmission practices and procedures.

(c) Request each government to examine this list to ensure that its own communications are free from such practices and procedures and invite additions to or comments on this list.

(d) Request each NATO government to designate or establish communications security agencies and to authorize those agencies to communicate directly with the Standing Group Communications Security and Evaluation Agency, Washington (SECAN) and the European Security and Evaluation Agency of the Standing Group (EUSEC).

(e) Invite any government that desires advice and technical assistance in such matters to apply, in the first instance, through their national communications security agencies directly to SECAN. Subsequent discussions or correspondence might be conducted, if more convenient, with EUSEC.

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 and of assuring each other that the communications security practices of their own nations are above reproach if judged from the standpoint of the agreed memorandum.

6. If the French Government agrees to these proposals, the U.S. and U.K. Governments will designate respectively one of their representatives on the Tripartite Security Working Group who has previously participated in the work of that Group to make the necessary arrangements in their behalf for the conduct of such discussions; and they suggest that the French Government similarly designate one of its experienced members of the Tripartite Security Working Group to join his U.S. and U.K. colleagues in making these arrangements. These arrangements would include agreement on the selection of the technical personnel, the location for the discussions and the establishment of proper conditions of security. This procedure takes advantage of an existing and very successful liaison channel in the field of security; and for added privacy it is proposed further that the necessary arrangements be worked out by our representatives without adding this matter to the formal terms of reference of the Tripartite Security Working Group and without making it subject to plenary consideration by that body,

U.K. PROPOSED AMENDMENTS.

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.

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.K. and U.S. 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.K. and U.S. Governments believe that it is essential for the U.S., France and 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.

~~TOP SECRET~~

US/UK

BRIEF FOR DELEGATES TO TECHNICAL DISCUSSIONS.

U.S. VERSION.

1. General.

(a) It is essential that the U.K. and U.S. delegations meet and consult in the U.K. before the discussions with the French begin.

(b) In participating in the French discussions, the U.S. and U.K. delegates are bound by the report of the June Conference, a copy of which is attached hereto as Appendix A.

(c) It is impossible to cover every eventuality in advance; the best way of eliciting and developing certain points must be left to the discretion of the delegates within the agreed limits of disclosure (in particular paragraphs 10b and c of Appendix A. Techniques employed in cryptosecurity evaluations are cryptanalytic techniques within the meaning of paragraph 10c of Appendix A.). In addition, care must be taken to guard against disclosure of the extent of the UK-US COMSEC collaboration.

(d) Complete agreement between the U.K. and U.S. delegations is essential. If differences emerge in the course of the discussions, the disputed points should be passed over until the two delegations have privately resolved their differences.

(e) Should unresolvable differences arise between the U.K. and U.S. delegations, or should it become evident to either that for any reason the conference has reached a point where further discussions with the French would be profitless, the U.K. or U.S. delegation, (after consultation with the other), will, using some plausible excuse, ask for a recess and get further instructions from the Combined Working Group. The delegations are not empowered to terminate the conference, for any reason other than that its work has been completed, without instructions from their governments.

2. Guide to the Conduct of the Discussions.

(a) The ostensible purposes of the discussions are set forth in paragraph 5 of the Aide Memoire which is to be left with the French by the Ambassadors. A copy of this aide memoire is attached hereto as Appendix B.

(b) An agreed UK/US draft of the memorandum referred to in paragraph 5 of the Aide Memoire will be introduced at the first session of the discussions. A copy of this draft and its appendix "List of Dangerous Practices" is attached hereto as Appendix C.

(c) The final report of the conference shall include a memorandum agreed by the technical representatives of the three powers and a recommended arrangement for introducing the memorandum into the Standing Group.

(d) The real purpose of the discussions, in addition to the objects stated in Appendix B, is to initiate an improvement in French communication security practices. For this purpose it is necessary first of all to cause the French to realize that their COMSEC practices fail to meet a satisfactory standard of security in the eyes of their allies. This goal will be achieved in part in the normal course of preparing the memorandum to be issued by the Standing Group. However, the full extent of the insecurity of the French can be brought home to them only by the revelation to them of a reasonably complete set of minimum standards covering among others the systems and procedure that they use.

(e) The U.S. Delegation will have been provided with a suitable version of the Minimum Standards paper. At some natural point, after the beginning of discussion of the draft Standing Group memorandum, when the French delegation raised the question of the rationale for some restriction proposed by the U.K. and U.S., the U.S. delegates will make this document available to the other delegates as if it were one of the U.S. reference papers which they feel the others might just as well have, and which would in all probability represent the official position of SECAN.

(f) The U.K. and U.S. delegates, before the discussions with the French begin, will arrange the procedure for introducing the paper, bearing 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.

(g) The sequel will depend on the reaction of the French. It is to be expected that they will realize that their systems and procedures are much farther than they had thought from what the U.S. considers to be minimum standards. This should lead to the kind of discussion which will eventually attain the true end of the conference.

(h) If the French indicate a desire to discuss their own communications practices and procedures, such discussion should be encouraged.

(i) The French may volunteer to discuss their recent request of the U.S. for cipher equipments for their Foreign Office. If they do not, the U.S. delegates will at an early stage seek out the French delegates privately and ask them to introduce the subject, saying that, in the interest of making sure that the best practical help is provided inthe shortest possible time, British participation might be advantageous.

U.K. PROPOSED AMENDMENTS.

2

(d) Delete final sentence and add to penultimate sentence:-

Fr modifications

" .....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. "

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

(e) "Every effort must be made to induce the French to discuss their own cyphers, communications practices and procedures. ~~In moving from the above theoretical discussion 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 1(c) above.

~~TOP SECRET~~

U.S. VERSION.

3. Limits of Cryptographic Disclosure.

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

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

(2) The systems and equipments that by the time of the conference may have been approved ~~by the U.S.~~ 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 Hollerith, with the procedures and standards of checking;

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

[redacted]

4. Predictable Sources of Embarrassment.

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(b) COMSEC - It is possible that the French might ask, pointblank, "what are the principles of the cipher system used by the U.S. State Department, 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.K. and U.S.) 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 extensive, 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.K. and U.S. to know its details and the fact of its use, or the system is so generally common to cryptography as to make COMSEC judgment an obvious matter.

U.K. PROPOSED AMENDMENTS.

(2) Insert after U.S. ....."and U.K.".

(b) COMSEC - If the French ask, pointblank, questions about national cypher systems of the U.S. and U.K., a frank answer should, wherever possible, be given. If the reply to such a question should 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.

~~TOP SECRET~~

If accepted this would replace (e)(f)(g)(h)

DRAFT

(f) 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 these tripartite discussions.

~~TOP SECRET~~