~~TOP SECRET FROTH~~
~~SECURITY INFORMATION~~

MEMORANDUM

Subject: Agreed Portion of Brief for Approach to the French on Communications Security by US and UK Ambassadors.

1. The briefs for the US and UK Ambassadors shall both include the following items:

(a) The Report of the BRUSA Conference on the Communications Security of NATO countries, held in June 1953.

(b) The aide-memoire prepared for the approach to the French by the Combined Working Group.

(c) Paragraphs 5 and 6 of USCIB paper 29.1/1 - attached as Appendix A to this memorandum.

(d) Instructions on how to respond in the event the French bring up the de Vosjoli approach on cipher machines at the meeting with the ambassadors - attached as Appendix B to this memorandum.

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

2. The briefs may also include whatever additional matters are considered necessary for the individual ambassadors, as determined respectively by the Foreign Office and the Department of State.

~~TOP SECRET FROTH~~
~~SECURITY INFORMATION~~

~~TOP SECRET FROTH~~
~~SECURITY INFORMATION~~

23 179

2

2 December 1953

AIDE-MEMOIRE FOR THE FRENCH

1. The US and UK 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 US and UK Governments also are of the opinion that the French Government may have reached a somewhat similar conclusion independently. The US and UK 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 review the national communications practices of all NATO governments.

2. The problem is twofold, involving not only the security of ciphers but also the security of transmission practices. It is important to emphasize that technical experts have proven again and again that the enemy can obtain important information from the external appearance of messages, from the study of organization and procedures of wireless networks, from wireless direction-finding, from a study of messages sent in plain language and from a variety of other observations not related at all to the

complexity or simplicity of given ciphers, but rather to the manner in which even the most secure ciphers are handled. Therefore, even if all NATO government ciphers and equipment were theoretically unbreakable, the protection afforded by this fact could be lost through improper procedures; and mere cipher security is useless if it is not complemented by transmission security.

3. The US and UK Governments together believe that it is essential for the US, France and the UK to assure themselves that their own standards are the best currently attainable if steps are to be taken with respect to the communications security practices of the other member governments of NATO. The UK and US Governments are conscious of a number of weaknesses in their own national communications practices. The French Government may also have noted similar weaknesses in their own practices. The Governments of the US and UK propose, therefore, that technical discussions among the communications security experts of the three Standing Group powers be held forthwith with the object not only of ensuring that the national communications practices of the three powers are of a level that is mutually agreed to be satisfactory but also as an

indispensable step in the development of similar standards for their colleagues in NATO.

4. If the French Government agrees to this proposal, the US and UK 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 US and UK colleagues in making these arrangements. These arrangements would include 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 Tripartitie Security Working Group and without making it subject to plenary consideration by that body.

5. It is the view of the US and UK Governments that the problem of the communications security practices of the remaining NATO governments should then 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.

6. On the assumption that the French Government agrees to the technical discussion as arranged by the Tripartite Security Working Group representatives, it is further invited to agree that, shortly after these discussions have been initiated, the Standing Group will issue a memorandum to all member governments of NATO which will:

~~TOP SECRET - SECURITY INFORMATION~~

(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 (EUSCE).

~~TOP SECRET SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

(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.