

~~TOP SECRET~~~~APPENDED DOCUMENTS
CONTAIN CODE WORD MATERIAL~~

USCIB: 29.1/6

20

15 December 1953

~~TOP SECRET~~MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Program to Improve the Communications Security of NATO Countries.

Reference: USCIB 29.1/1 of 21 September 1953.

1. The enclosed papers designed to guide implementation of the program outlined in paragraph 6 of the reference are submitted by the Chairman of the USCIB Ad Hoc Committee for this problem (Mr. T. A. Polyzoides) in order to obtain the formal approval of USCIB to go ahead with the program.

2. Attention is invited to paragraph 1e of enclosure 5 (Brief for Delegates) wherein it is provided that the CWG be the source of instructions to the U.S. and U.K. delegates during the course of discussion. The CWG recommends this procedure as being the most efficient and effective manner in which to resolve U.S.-U.K. differences that may arise during the course of the discussions. In this connection attention also is invited to the following provisions of the reference approved by USCIB as guidance to the U.S. Ad Hoc Committee:

"4. The Combined (US-UK) Working Group. To assure that the COMINT aspects and limitations of this program are properly coordinated, the Combined Working Group should be under the direction of USCIB and LSIB. It should serve to:

a. Coordinate US and UK proposals for the initial approach to the French, subsequent technical discussions, preparation of a memorandum to be issued by the NATO Standing Group and formulation of minimum security standards;

b. Coordinate, between the US and UK, conclusions as to the status of the COMSEC of NATO countries as this program develops; and

c. Coordinate US and UK recommendations for further steps, as envisaged in paragraph 23 of the Conference Report, should this program not accomplish the desired response from NATO countries or improvement in their COMSEC.

The US element of this Group should also serve as an ad hoc sub-committee of USCIB to keep this entire program under continuous review for the Board."

USCIB: 29.1/6

~~TOP SECRET~~~~APPENDED DOCUMENTS
CONTAIN CODE WORD MATERIAL~~

54-770

USCIB: 29.1/6

15 December 1953

~~TOP SECRET~~

Subject: Program to Improve the Communications Security of
NATO Countries.


"6. - - - -

c. Phase 3. The COMSEC authorities should then proceed to the discussion and implementation of adequate COMSEC practices within the three Governments. US participation in this phase should be handled by the National Security Agency (NSA)."

The Chairman of the U.S. Ad Hoc Committee foresees no difficulty in adjusting those matters which would be handled by the CWG during the course of the discussions and those that would be handled by the National Security Agency inasmuch as problems to be settled by the CWG would be received at NSA from the U.S. delegates and tabled through the NSA members of the CWG. Likewise problems arising in the U.K. delegation would be passed to the U.K. element of the CWG via London.

3. The Chairman of the U.S. Ad Hoc Committee recommends approval of the enclosures. Such approval should be construed to include re-affirmation by USCIB of the fact that policy aspects of the subject program will continue to be referred to the CWG until the program is completed. In order to expedite action and save unnecessary consideration of detail by the Board it is recommended that the U.S. element of the CWG be authorized to negotiate any further changes desired by the U.K. to the enclosures without reference to the Board provided such action involves no change in the essential requirements of the program as embodied in the reference and the enclosures hereto. It is suggested that the Board's views on ~~these~~ points be conveyed to LSIB.

these


RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosures

1. Chr. Ad Hoc Cte. Memo of 15 Dec 1953. *Rev. 3 Feb. 54*
2. Brief for Approach to the French on COMSEC.
3. Aide-memoire for French-dtd 10 Dec-1953. *Rev. 3 Feb. 54*
4. Agenda Mtg. Delegates Tripartite Sec. Work Group.
5. Brief for Delegates Technical Discussions, 10 Dec 1953. *Rev. 3 Feb 54*
6. Memo for Standing Group to Issue of 23 Nov 1953.
7. Lists of examples of dangerous crypto and comm. practices.

USCIB: 29.1/6

- 2 -

~~TOP SECRET~~

~~TOP SECRET~~

MEMORANDUM FOR THE CHAIRMAN, USCIB:

Subject: Program to Improve the Communications Security
of NATO Countries.

Reference: USCIB 29.1/1 of 21 September 1953.

1. Under the terms of the reference document, an Ad Hoc Committee representing USCIB has been working as the U. S. element of a Combined (US/UK) Working Group (CWG) to coordinate U. S. and U. K. proposals for the initial approach to the French and for other matters connected with the program to improve communications security of NATO countries.

2. The deliberations of the USCIB Ad Hoc Committee and the CWG resulted in early agreement that the task at hand required a mutually agreed sequence of four major steps which in turn would require a certain number of agreed documents of instruction and guidance. It was also agreed that USCIB and LSIB should reach agreement on the entire series of these documents before an approach to the French was made.

3. The attached documents comprise the series deemed to be the necessary preparation for the initial approach to the French and for subsequent conferences as required. The Ad Hoc Committee has approved this series unanimously. The British element of the CWG has participated throughout in the preparation of these documents and has approved them subject to final approval from London. / ||

4. The Committee recommends that the Board (a) approve the attached series of papers as the formal U. S. position for initiating the approach to the general program; (b) direct the Ad Hoc Committee to complete the necessary negotiations and adjustments with the British element in the CWG without further reference to the Board, unless disagreements over matters of policy cannot be resolved within the CWG; and (c) reaffirm that policy aspects of the subject program will continue to be referred to CWG until the program is completed.

(Signed)

T. Achilles Polyzoides
Chairman, Ad Hoc Committee

Enclosure 1 with USCIB 29.1/6 (Revised as of 3 February 1954)

~~TOP SECRET~~

~~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.
- (e) ~~The US and UK agree that no revelation of US and/or UK [redacted] will be made to the French at the ambassadorial level. Revelation within the limits set forth in the conference report (See paragraph (a) above) will be reserved for the technical discussions themselves.~~

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~~

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

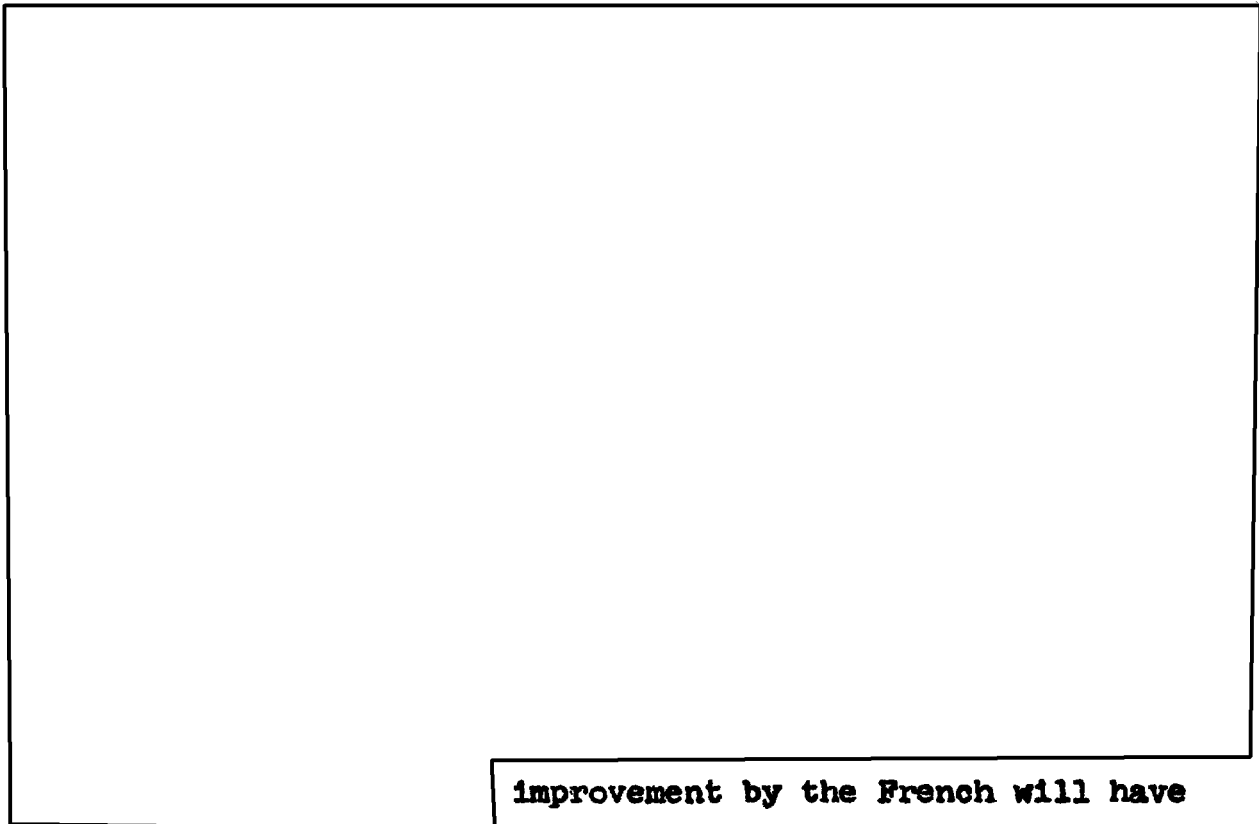
~~TOP SECRET FROTH~~
~~Security Information~~

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

APPENDIX A

Paragraphs 5 and 6 of USCIB 29.1/1

5. Considerations affecting the initial approach to the French.



improvement by the French will have to be achieved indirectly, i.e., by inducing them to agree first to a program for the improvement of the COMSEC of NATO countries through the existing COMSEC mechanism of the NATO Standing Group and then to agree to preliminary US-French technical discussions to assure adequate COMSEC practices within the three governments.

~~TOP SECRET FROTH~~
~~Security Information~~

~~TOP SECRET FROTH~~
~~Security Information~~

c. It will be imperative that all contacts made within the French Government are secure and are given adequate authority.

d. The Tripartite Security Working Group (US-UK-French), which has been in existence since 1950, would appear to offer the best means of achieving an orderly and secure arrangement for direct discussion between the proper COMSEC authorities of the three governments. Although the work of this Group has not heretofore included COMSEC matters, the Group has developed cooperative and secure contacts among responsible French authorities in general security matters.

6. The initial approach to the French. To assure wholehearted cooperation by the French in sponsoring jointly with the US and UK the overall program for other NATO countries and in making effective improvements in French COMSEC, the French Government should be approached first at the cabinet level. The project should then be assigned to the Tripartite Security Working Group to establish proper contact between COMSEC authorities of the three governments. As a practical matter, and as a means of achieving the greatest possible compulsion, this approach should be undertaken jointly by US and UK representatives.

-2-

~~TOP SECRET FROTH~~
~~Security Information~~

~~TOP SECRET FROTH~~
~~Security Information~~

a. Phase 1. At the cabinet level the French Government should be requested by the US and UK ambassadors to agree in principle that the overall security of NATO requires that a broad program be undertaken to improve the security of the national communications of NATO countries, and that this program should be initiated through the Standing Group as a logical extension of the existing COMSEC program of the NATO organization itself. The French Government should be requested to agree further that such a program should be preceded by US-UK-French discussions to assure adequate COMSEC practices within the three Standing Group countries, and that, to this end, the terms of reference of the Tripartite Security Working Group should be extended to include the establishment of arrangements for technical discussions and the selection of competent and proper COMSEC authorities to undertake these technical discussions and implement their results within the three governments. This phase should be handled by the Department of State and the Foreign Office.

b. Phase 2. The Tripartite Security Working Group should then select the COMSEC authorities who will represent their Governments and make suitable arrangements for their

~~TOP SECRET FROTH~~
~~Security Information~~

~~TOP SECRET FROM~~
~~Security Information~~

technical discussions. This phase should be handled by selected members of the US and UK Tripartite Security Teams as agreed between the participating agencies.

c. Phase 3. The COMSEC authorities should then proceed to the discussion and implementation of adequate COMSEC practices within the three Governments. US participation in this phase should be handled by the National Security Agency (NSA).

~~TOP SECRET FROM~~
~~Security Information~~

~~TOP SECRET - SECURITY INFORMATION~~

APPENDIX B

Instructions on Response to any French Reference
to Cipher Machine Approach to US

1. It is considered unlikely that during conversations with the US and UK Ambassadors the French will mention the fact that they have approached the US with a request for cipher machines. If they should do so, no indication should be given that the US has told the UK of the request.
2. The US Ambassador should say (a) that he was informed of the French approach; (b) that it is under consideration in Washington; and (c) that he believes the matter would be taken up at some point in the proposed technical talks, if they are agreed to.
3. The UK Ambassador should remain silent or if necessary should (a) say that he was not aware such an approach had occurred; (b) ask to be informed of pertinent details of the request; and (c) if the French approach is described, agree that the matter appears to fit into the proposed technical talks.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET~~~~TOP SECRET~~

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 bring this situation to the attention of all NATO governments.

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.

3. It is the view of the US and UK 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

Enclosure 3 with USCIB 29.1/6 (revised as of 3 February 1954)

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

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 US and UK Governments together believe that the US, France and the UK 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 these 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.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

5. 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 of agreeing upon a memorandum for issue by the Standing Group to all NATO governments. The UK and US Governments are, however, conscious of a number of shortcomings in their own national communications practices: The French Government may also have noted similar shortcomings in its own practices. The US and UK Governments believe that as a further objective of the technical discussions the US, UK and France should assure themselves that their respective communications security practices are satisfactory from the standpoint of the Standing Group Memorandum.

6. If the French Government agrees to these proposals, 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 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 the Tripartite

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

Security Working Group and without making it subject to plenary consideration by that body.

~~TOP SECRET~~

~~TOP SECRET - SECURITY INFORMATION~~

AGENDA AND BRIEF FOR THE MEETING
OF DELEGATES FROM THE TRIPARTITE
SECURITY WORKING GROUP

- (1) A designated representative of each country on the Tripartite Security Working Group who has previously participated in the work of that group will meet in Paris as soon as is practical and possible after agreement has been reached among the three governments relative to taking the action proposed on communications security. (Holding of the meetings in Paris will facilitate action of the group inasmuch as it is anticipated the French delegate will have to refer to other governmental agencies prior to consummation of the arrangements for a meeting of the technical group, whereas the British and U.S. delegates should be thoroughly prepared to enter into any necessary commitments. Also, the security checking relative to the French delegates will be facilitated if the meetings are in Paris.)
- (2) The action to be proposed at the meeting of the Tripartite Security Working Group representatives will be as follows:
 - (A) There should be a discussion of the problem involved with security emphasis (this is to insure that the French representative is properly briefed inasmuch as he may have had scanty information up to this time).

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

- (B) Discussion will be initiated as to the security aspects of the meeting of the technical delegates which would cover security protection, physical security, and any other security problems.
- (C) Each of the delegates will table the names of their technical representatives proposed for the technical meeting for scrutiny, checking and discussion with the other two delegates.
- (3) It is proposed that two competent technical representatives be designated from each country to participate in the technical meetings. This would permit additional representatives if it proved necessary after the initial meeting. The technical committee would hold their meetings in Paris (if this proves not to be feasible, then in London) as soon as is possible and practical after the Tripartite Security Working Group representatives conclude their work. In any event, it would be proposed that the meeting of the technical representatives start within thirty days (this would seem to be chiefly a problem for the French inasmuch as the U.S. and British technical teams will be ready to meet at any time).

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET~~~~TOP SECRET~~

BRIEF FOR US-UK DELEGATES TO TECHNICAL DISCUSSIONS

1. General.

- a. It is essential that the UK and US delegations meet and consult in the UK before the discussions with the French begin.
- b. In participating in the French discussions, the US and UK 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 UK/US COMSEC collaboration.
- d. Complete agreement between the UK and US 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 UK and US 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 UK or US 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

Enclosure 5 with USCIB 29.1/6 (revised as of 3 February 1954)

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

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 the 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 communications 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 and in discussion of its Appendix: List of Dangerous Practices. French recommendations for modifications, especially amplification, will be encouraged and considered on their own merits. Decisions on these points must necessarily be unanimous.

e. Every effort must be made to induce the French to discuss their own ciphers, communications practices and procedures. The exact

~~TOP SECRET~~

~~TOP SECRET~~

tactics will be agreed between the US and UK 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-paragraph 1(c) above.

f. The following device may be used if at any stage it appears to both the UK and US delegates that it will further the real purpose of the discussions. The US 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 UK and the US, or when some basis is required for a statement in the "List of Dangerous Practices", the US will make available to the other delegates either the whole of this document or relevant sections, as if it were one of the US 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 UK and US 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~~~~TOP SECRET~~

g. The French may volunteer to discuss their recent request of the US for cipher equipments for their Foreign office. If they do not, the US delegates may 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 in the shortest possible time, British participation might be advantageous.

3. Limits of Cryptographic Disclosure.

a. The disclosure of US or UK 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 for release to the French as a result of their request for assistance for their Foreign Office;
- (3) The UK method of making one-time pads by HOLLERITH, with the procedures and standards of checking;
- (4) The UK method of making one-time tapes by DONALD DUCK (with a statement that US methods are similar) and the procedures and standards used for checking.

b. The disclosure of non-US or UK cryptographic detail shall be limited to that which is available only from non-COMINT and overt sources.

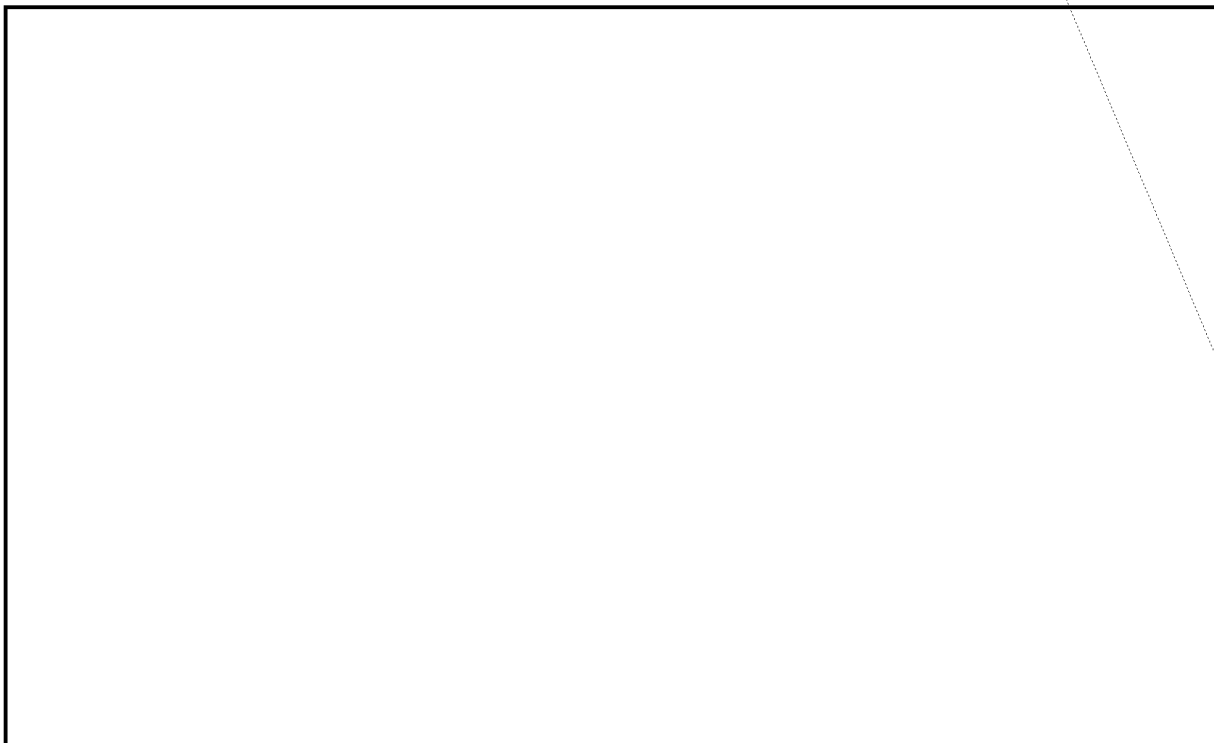
~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

taken to avoid the use of any words or phrases peculiar to French communications which are known to us through COMINT for example "Omnice," "Boite de Roulette," "Avec mit," and the like; it must be borne in mind at all times that words which have become commonplace technical terms can provide direct evidence of COMINT success or collaboration.

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

4. Predictable Sources of Embarrassment.



b. COMSEC - If the French ask pointblank questions about national cipher systems of the US or UK, a frank answer should wherever permissible, be given. If the reply to such a question should involve revelation of matter not approved for release, the answer should simply be that each country has a national security policy which prohibits revelation of such information except as explicitly approved.

~~TOP SECRET~~

~~SECRET - SECURITY INFORMATION~~

25 November 1953

MEMORANDUM FOR STANDING GROUP TO ISSUE

1. Regulations at present in force (DC 2/7 (Final) and STAND 474 as amended by STASECS 1508, 1535 and 1588) ensure that all COSMIC telegrams and all NATO TOP SECRET and SECRET telegrams are encyphered in cryptosystems authorized by the Standing Group. But all nations of NATO are also originating and transmitting in their own national cryptosystems a quantity of telegrams both civil and military which, although they are the private concern of the nation in question, must be expected to contain information which affects NATO as a whole and the loss of which to a non-NATO nation harms the security of NATO.
2. Further STAND 474 allows NATO telegrams graded CONFIDENTIAL OR RESTRICTED to be encrypted in national systems, and it is highly undesirable that information of such gradings should become available to nations outside NATO.
3. The Standing Group therefore feels considerable concern at the potential danger to the security of NATO which may arise from the insecurity of the national communications of individual nations: the insecurity of one can endanger the security of all.
4. The Standing Group has had prepared a paper enumerating examples of cryptographic and communications practices and procedures which endanger security. This paper is attached at Appendix A. The Standing Group requests that each member nation examine this paper and take action to ensure that its own communications are free from the practices and procedures mentioned therein.
5. Further the Standing Group requests that each NATO nation will designate or establish a Communications Security Agency which shall be authorized to

Enclosure 6 with USCIB 29.1/6

~~TOP SECRET~~~~SECRET - SECURITY INFORMATION~~

communicate on communication security matters both civil and military direct with the Standing Group Communications Security and Evaluation Agency Washington (SECAN) and with the European Security and Evaluation Agency (EUSEC).

6. The Standing Group invites any member nation, which requires advice and technical assistance towards the improvement of the security of its national cryptographic and communications practices and procedures whether civil or military to apply through their Communications Security Agency direct to the Standing Group Communications Security and Evaluation Agency Washington. It may subsequently be found more convenient for SECAN to arrange for discussions arising out of this first approach to be held with EUSEC.

~~TOP SECRET~~

~~TOP SECRET SECURITY INFORMATION~~

25 November 1953

LIST OF EXAMPLES OF DANGEROUS
CRYPTOGRAPHIC AND COMMUNICATIONS
PRACTICES AND PROCEDURES

I. UNENCIPHERED CODES.

1. Unenciphered codes are totally unacceptable in diplomatic use for transmission of classified information. They are only acceptable for Armed Forces communications when it is not considered essential to maintain the security of the information for more than two or three days from the introduction of the code. It follows that such codes must be changed at very frequent intervals.

II. ADDITIVE SYSTEMS

2. Any additive (or subtractor or minuend) system is dangerous unless special precautions are taken in the construction of the additive itself. Many procedures that may be regarded as "special precautions" are deceptive as to security and may even in themselves create weaknesses.

3. Encipherment by additive can only be guaranteed to be secure when the additive is used on a strictly "one-time" basis, and systems that permit depth gain little or no security from the additive.

4. Encipherment by non-one-time additive is highly dangerous, but can be acceptable in certain circumstances for limited traffic provided that precautions are taken to minimize overlap and to prevent cryptanalysts from finding any overlap that may arise.

5. In general, polyalphabetic substitution systems whether actually additive in nature or not, are like additive systems and are subject to the same dangers.

Enclosure 7 with USCIB 29.1/6

~~TOP SECRET - SECURITY INFORMATION~~

III. NON-ADDITIVE HAND SYSTEMS

6. There are many hand systems of encipherment that do not employ additive. Very few of these can be guaranteed to be secure, even though they may be very complex, applying both substitution and transposition to code or plain language.

IV. MACHINE SYSTEMS

7. Machine ciphers vary greatly in the amount of security they afford. Failure to observe in every detail proper instructions for operation may lead to compromise even with the best machines. Others, such as the well-known Hagelin "Cryptoteknik" (see para 8 below) are insecure unless precautions are taken over and above those recommended by the manufacturer. Others, again, are basically insecure and should in no circumstances be used.

a. Since the encipherment is essentially by additive, it follows that if a message setting is used more than once the key can be recovered on the overlap; a single mistake by an operator using a message setting a second time can thus compromise the machine setting.

b. The additive generated by the machine is never truly random and there are circumstances in which this fact can be used to recover the machine setting, even though no message setting is repeated.

c. With proper precautions this machine can give very good security for a limited amount of traffic, but in view of the number of different dangers that can arise in varying conditions of use, for which it is impossible to legislate in advance, member nations who wish to make use of the "Cryptoteknik" are especially urged to consult SECAN.

~~TOP SECRET - SECURITY INFORMATION~~

V. TRANSMISSION SECURITY.

9. Ciphers, however good individually, are not enough to ensure communications security. Transmission techniques and message formats can in themselves provide considerable intelligence to a traffic analyst. Although there are practical limitations, the ideal to be striven for is that the traffic neither of any type (e.g., naval, air force, etc.) nor of any nation should be distinguishable by external characteristics. Again, intelligence can be gained by study of the organization and procedure of radio networks and by use of radio direction-finding. In many cases, especially in Armed Forces communications, a skillful enemy can obtain valuable intelligence by collation of apparently uninformative message texts. It follows, therefore, that full communications security demands that special precautions be observed in such matters as the judicious employment of indicators, the selection of call signs and of frequencies, radio procedures, and the restriction of the use of plain language.