23 January 1951

MEMORANDUM FOR MEMBERS OF THE AD HOC COMMITTEE:

Subject: Status of French Security Problem.

1. The following is a brief resume of the recent actions taken in the subject problem. Pertinent enclosures are included to provide more detailed information:

a. History of the Problem: In 1948, USCIB discussed the problem of French security, as the most important aspect of a consideration of the "Security of Western European Union Communications". At that time it was realized that vital information was being turned loose as a result of the faulty security practices and procedures employed by the French. The problem was studied by an Ad Hoc Committee which made its report to USCIB. USCIB could not reach agreement and submitted a split report to the National Security Council (NSC) - the majority (ID, ASA, CNC, and CIA) feeling that too much would be lost. [redacted] NSC voted to take no action at that time, but directed that the problem be kept under surveillance.

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

b. Subsequent Actions: The problem was presented to USCIB again at the 55th Meeting, 15 September 1950, when Admiral Hillenkoetter raised the question, and Mr. Armstrong discussed the matter informally and informed the members that the seriousness of the French Security problem had reached such proportions that a reconsideration was necessary. Mr. Armstrong's comments at this meeting are attached as Tab A.

(1) USCIB agreed that the problem should be referred to SECCOM for urgent consideration and recommendation.

(2) SECCOM submitted an interim report (Tab B), which was discussed briefly at the 56th Meeting (Tab C).

(3) At the 57th Meeting, 10 November 1950, USCIB considered the final report of SECCOM and made certain amendments thereto. The USCIB discussion of this report, and the amended report, in full, are attached as Tab D.

23 January 1951

Subject: Status of French Security Problem.

(4) At the 58th Meeting, 8 December 1950, the Board designated the Coordinator (See Tab E) as the USCIB representative:

(a) To coordinate with the U.S. negotiators on this problem (Col. H. H. Howze (G-2) and Mr. Fisher Howe (State)).

(b) To work out a U.S./U.K. position on the matter with Brigadier Tiltman.

c. Up to this point there had not been U.S./U.K. discussions on the matter. On 8 January 1951 USCIB members received copies of a letter from the Chairman, London Sigint Board on this subject (Tab F), stressing the need for prompt action and asking for a U.S./U.K. conference on the subject early in 1951. USCIB discussed this letter at the 59th Meeting, 12 January 1951. It was agreed to send a reply to the Chairman, LSIB which would not accept all his specific proposals, but which would agree upon an early conference (about 1 April 1951) on the problem and inform him that AFSA would proceed to prepare a U.S. position in the matter in accordance with paragraph 7(c) of the LSIB letter. USCIB agreed, further, to advise LSIB that the U.S. favored consideration of the problem on a broad (all aspects of French security) basis rather than on a basis of diplomatic cryptosystems alone.

2. The above outlines the French Problem in general terms. In review, the present status of the problem is as follows:

a. <u>On the strictly U.S. side</u>:

(1) USCIB has approved the SECCOM report, which will serve as a U.S. position for the "negotiators" (Col. Howze and Mr. Howe) in the event of high-level (Bradley-Tedder-Moch) discussions on the French situation.

23 January 1951

Subject: Status of French Security Problem.

(2) There is no indication when such discussions will be held. The negotiators will inform the USCIB Coordinator.

b. On the U.S./U.K. side:

(1) USCIB has agreed to a conference on the subject, to be held about 1 April 1951.

(2) The Ad Hoc Committee has been directed to prepare a U.S. position on the French problem, for consideration by USCIB, to serve as a U.S. basis at the above conference.

H. B. JONES
Secretary, Ad Hoc Committee

Minutes of an Informal Discussion at the Fifty-Fifth Meeting of USCIB, 15 September 1950, on the subject of The Cryptographic Security Practices and Procedures of Certain Western Union Nations.

MR. ARMSTRONG announced that the Director of Central Intelligence had requested permission to present an item not on the agenda for this meeting. He asked Admiral Hillenkoetter to proceed with his presentation.

Tab A

ADMIRAL HILLENKOETTER stated that he wished to bring a matter to the attention of the Board, however he had no solution to suggest. He said that there had been several recent instances in which [redacted] He added that it might be fairly assumed that such information ultimately reached Russian hands.

ADMIRAL JOHNSON said that he had intended to raise a similar question in an executive session, which he had requested the Chairman to call at the end of the regular meeting.

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

After a brief discussion the members agreed that an executive session would not be required and that the matter could be brought up in open meeting. The Chairman agreed to review the problem briefly.

MR. ARMSTRONG recalled that this matter had been considered about two years ago at which time the Board forwarded a recommendation to the National Security Council (NSC) on the question of the advisability of informing the French of their cryptographic insecurity. He said that the NSC decision was to take no action at that time except to try to provide the French with facilities which would insure greater security. He said that this matter was studied as it pertained to the Western Union Organization, and, later, to the North Atlantic Treaty Organization (NATO); however, to date the situation has not been remedied.

MR. ARMSTRONG explained that French insecurity continued and, if anything, was continually causing a greater problem. [redacted]

MR. ARMSTRONG continued that he had explained to the Secretary of State that there was high-level Russian penetration in the French Government, which might nullify action taken to improve French cryptographic practices and procedures. He said that the Secretary had decided to raise the question with Secretary of Defense Johnson and General Bradley. Both had felt that there was little to be gained and that impatience at

this point would be of no avail. They had been of the opinion that it would be best to tackle the problem on a long-range basis and work from the ground up. As a result of the above, the Secretary of State decided not to pursue the matter further.

MR. ARMSTRONG, turning to another aspect of the problem, said that in August 1950, the British Ambassador had proposed, upon the recommendation of the British JIC, that the U.S. join with them in an effort to solve the problem. He said the British had found themselves in the embarrassing position of denying to the French information which the French knew about, in general, and on which they should have the details. The British had proposed a two-pronged attack: (1) Raise the problem with the French in a standing group of NATO and ask them to join with the U.S. & British in security enforcement - a move which would result in codifying security practices from the ground up, and (2) Have the U.S. and British ambassadors in Europe go to the top French Government officials and ask them to do all they could toward insuring strict enforcement of security principles.

PL 86-36/50 USC 3605

MR. ARMSTRONG continued by saying that at about the same time of the above discussions [redacted] had approached General Bradley on the subject. He said that in these discussions we had suggested a different solution, namely, that the matter of standardization of security regulations, development of equipment, etc. be discussed with Jules Moch, who would be able to get together a small group of cleared, competent individuals who could be trusted, and who would compose a group which could be reached. He said that the British had agreed to this approach and that our ambassador had gotten a cordial reception in his first discussions with Moch on 12 September. The State Department has asked the Department of Defense to designate an office or agency to handle these negotiations as, primarily, a military matter.

MR. ARMSTRONG explained that though these discussions with Moch were on a broad scale, the subject of communications would come up sooner or later, probably after the adoption of basic security practices. He added his assurance that the military departments would hear from the JCS on this subject in the near future, if they have not already been approached.

[redacted]

ADMIRAL HILLENKOETTER commented that providing secure cryptographic means to the French would have the effect of [redacted]

GENERAL CABELL agreed that there would be a net loss, however he expressed his opinion that an increase in French cryptographic security should be sought, [redacted]

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

ADMIRAL STONE said that he would support that view. He added that he could not concur with the oft-expressed opinion that the French had only insecure systems. He said that they did not use their secure systems at times when they should have - from our viewpoint. He suggested that measures should be taken:

(a) To insure that the French and others concerned be required to use one-time pad systems in international conference reporting, where U.S. is taking part in the conference.

(b) To plan on a long-range basis, to improve and make secure the diplomatic communications of all allied nations.

GENERAL CABELL proposed that the Board restudy the question of French cryptographic security which was studied two years ago.

MR. ARMSTRONG agreed with this proposal. He commented that if French cryptosecurity were to be improved it should be improved "across the board".

ADMIRAL JOHNSON agreed with General Cabell that what would be lost by improving French Security would be negligible when compared with what would be gained.

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

ADMIRAL STONE agreed, stating his belief that the matter probably could be handled without causing too much [redacted] He mentioned again the great need for achieving security in connection with international conferences involving the U.S.

ADMIRAL REDMAN commented that if it was ever decided to tell the French that their systems were no good, it would be a good time to feed the Russians deception material.

MR. ARMSTRONG asked if the French military cryptosystems weren't reasonably secure.

ADMIRAL STONE replied that they had some secure systems and were sophisticated in crypto-security knowledge. He added that the French had a secure high-level diplomatic system, which they didn't use at times when it appeared they should. He indicated that they may have a philosophy about using their weak and their secure systems which we do not understand.

COLONEL PETERSON stated that he had discussed this matter with the technical experts, all of whom felt that the French were intelligent enough, cryptographically, to know what they were doing. He said that it was evident that the French had some good systems and that they were pursuing a cryptographic policy; however, that policy seemed to be to use a poor system in order to protect a good one.

ADMIRAL STONE agreed, and said that it seemed they might intentionally refrain from using a highly secure system for transmitting information which could be expected to appear in the newspapers the following day.

MR. ARMSTRONG asked if the members were agreed that this matter should be referred to a committee for urgent study.

The members agreed.

MR. ARMSTRONG asked if it was desired that the problem be studied by an Ad Hoc, or an existing, committee.

The members agreed that the matter would be referred to the Security Committee.

ADMIRAL JOHNSON asked if it were known whether or not the Secretary of Defense and General Bradley were firm in their opinion that little could be gained on other than a broad-based approach to the problem.

MR. ARMSTRONG said that he thought their opinions would be subject to change if they were presented with what appeared to be a workable plan.

[redacted] be considered. He recalled that such a plan had been used successfully in the Pacific during World War II.

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

There were no further comments.

DECISION: USCIB agreed that the Security Committee would be directed to re-study, as a matter of urgency, the general problem of the insecurity of French cryptographic practices and procedures which had been considered by the Board in the fall of 1948. It was agreed, further, that the Security Committee would (a) Determine, on the basis of the 1948 study and events happening since that time, whether any action toward improvement of French cryptographic practices and procedures is deemed advisable, and (b) Recommend, if the answer to (a) is affirmative, proposed corrective measures for USCIB implementation.

~~TOP SECRET~~

APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL

USCIB: 14/93

11 October 1950

MEMORANDUM FOR MEMBERS OF USCIB:

Subject: Security of Foreign Communications.

1. The attached interim report from the Chairman, Security Committee, above subject, is forwarded for your information.

2. This report will be considered under Item 4 of the final agenda for the Fifty-sixth Meeting of the Board, 13 October 1950.

H. D. Jones

H. D. JONES
J. W. PEARSON
Secretariat, USCIB

Tab B

APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL

USCIB: 14/93

~~TOP SECRET~~

DEPARTMENT OF STATE
WASHINGTON

10 October 1950

MEMORANDUM FOR THE CHAIRMAN, USCIB

SUBJECT: Security of Foreign Communications

Reference is made (a) to the informal discussion of this matter, with particular reference to the French, which was held at the close of the Fifty-fifth Meeting of USCIB on 15 September 1950 and (b) to the decision of the Board that the entire problem should be referred to SECCOM for further study and recommendations.

SECCOM is now considering as a matter of urgency, whether it would be advisable to take action toward the improvement of French communications security practices and procedures and, if so, what should be the nature and scope of corrective measures to this end. It is expected that the final recommendations with regard to these questions will be forwarded to USCIB prior to 31 October. The Chairman, SECCOM will be prepared to present a verbal progress report of these considerations at the next meeting of USCIB.

In view of the program which is now underway within the Departments of State and Defense directed toward the overall problem of French security, SECCOM recommends that, as a matter of urgency, USCIB approve and forward the following recommendations to those authorities within the Departments of State and Defense who are responsible for the development of this program:

a. That, inasmuch as the problem of overall French security involves the security of French communications and the availability of these communications [redacted] all US and UK personnel assigned specifically to participate in US-UK or tripartite negotiations affecting French security should be indoctrinated for COMINT and should be briefed thoroughly as to the problems of (1) the insecurity of French communications and its effect upon the security of the US and (2) French communications security and its relation to the [redacted]

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

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

SECCOM ITEM No. 133

USCIB will, in the near future, present specific recommendations with regard to these matters.

b. That the question of French communications security should not be placed on the agenda for the first discussion with the French and should not be included in subsequent agenda until such time as discussion and improvement of other security matters have demonstrated that the French have made definite progress toward overall security.

c. That, in the event that this problem is raised by the French prior to being placed on the agenda for discussion, its consideration should be postponed on a "No comment" basis.

OGA

[redacted]

Chairman, USCIB Security Committee

FINAL

SUBJECT NUMBER

USCIB: 14/95 Item 4 of the Agenda for the Fifty-sixth Meeting of USCIB, held 13 October 1950.

Subject: Security of Foreign Communications.

MR. ARMSTRONG referred to USCIB: 14/93 and informed the members that it contained an interim report from the Chairman of the Security Committee on the French Security problem. He recalled that the Board had, at its last meeting, given the problem to SECCOM for study. He then invited Mr. Collins, Chairman of SECCOM, who was present at the meeting, to comment further.

[redacted] said that in addition to the recommendations contained in the memorandum for the Chairman, USCIB, dated 10 October 1950, the SECCOM, at a subsequent meeting, had recommended that, should discussions with the French involve matters within the cognizance of USCIB at some later date, USCIB should designate an official to represent USCIB, along with the U.S. negotiators, to determine (a) the most feasible approach to be used and (b) the degree to which it may be necessary to [redacted] He added that the SECCOM further recommended that the Board ask the appropriate authorities handling these negotiations for the State and Defense Departments to make no approach along these lines without the advice or concurrence of USCIB's representative.

Tab C

OGA

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

MR. ARMSTRONG asked for comments.

ADMIRAL JOHNSON made reference to items (1) and (2) contained in subparagraph a. at the bottom of page one of the interim report (USCIB: 14/93). He said that he was in agreement with item (1), but would like clarification of item (2). It was his understanding, he said, that this item concerned the [redacted]

[redacted] replied that this understanding was correct, whereupon ADMIRAL JOHNSON expressed his opinion that the [redacted] was, in reality, a very minor consideration.

MR. ARMSTRONG asked Mr. Collins if his committee had considered the matter with this thought in mind.

[redacted] replied in the negative, and went on to state that some of the preliminary decision of his committee included the following principles:

USCIB: 14/95

[redacted]

2. SECCOM feels that, to the extent that active collaboration between the U.S. and France becomes close and effective, the dangers to the security of the U.S. through insecurity of French diplomatic traffic will outweigh [redacted]

3. In the light of general French insecurity, the immediate advantages accruing to the security of the U.S. by urging improvement in the cryptographic security of French diplomatic traffic are outweighed by the current and potential value of [redacted]

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

4. However, if U.S.-French collaboration is expected to become so close as to require eventual improvement of the security of French diplomatic revelations, immediate steps toward this improvement would entail a potential advantage which might outweigh the value of the [redacted] which might be lost thereby.

In other words, he said, under current thinking the [redacted] outweighed security considerations.

ADMIRAL JOHNSON said that he understood that the reason for taking no action two years ago was because of probable [redacted]

MR. ARMSTRONG stated that this was not entirely true. He said that, in fact, the Board's final majority opinion on the subject was that the [redacted] was outweighed by the loss of security.

MR. ARMSTRONG added that he might comment further upon more recent developments regarding steps now under way toward the improvement of overall French Security. He then reviewed briefly these developments.

USCIB: 14/95

GENERAL BOLLING said that there was a possibility that Moch would remain in this country until General Bradley returned, in which case there might be an opportunity for a Bradley-Tedder-Moch discussion.

MR. ARMSTRONG commented that such a conference was much to be desired. He asked for any further comments.

There were none.

DECISION: USCIB noted the interim report by the Security Committee as contained in USCIB: 14/93.

This item to be continued on the agenda.

SUBJECT NUMBER

USCIB: 14/100 Item 3 of the Agenda for the Fifty-seventh Meeting of USCIB, held on 10 November 1950.

Subject: French Diplomatic Cryptographic Security.

MR. ARMSTRONG introduced this item and explained that it involved consideration of the SECCOM report on the subject which was circulated under date of 3 November 1950. He informed the members that the Chairman of SECCOM was present, and might wish to comment on the report.

[redacted] said that he had nothing to add to the report, but would be glad to answer any questions.

OGA

MR. ARMSTRONG asked for comments on the report.

ADMIRAL JOHNSON said that he had several amendments to propose.

MR. ARMSTRONG said that before the amendments were considered he would like to ask if the Board wished that the report go to the National Security Council (NSC) now, or be held until later. He explained that the discussions on the French security problem had not yet reached the communications phase, and the members might wish to have the NSC consider the report closer to the date that the communications problem comes before it. He asked if the Army was anxious to have action taken at this time.

COLONEL HOWZE replied that action was not necessary until the question of basic French security had been settled.

Tab D

ADMIRAL JOHNSON suggested that the report be sent to NSC in order to acquaint them with the seriousness of the problem.

GENERAL CABELL said that he thought it would be best to leave the decision to the discretion of the negotiators who would be primarily concerned with the problem.

DR. CRAIG and MR. KEAY agreed with General Cabell.

ADMIRAL JOHNSON said that he did not feel strongly about having the report forwarded now.

MR. ARMSTRONG then asked if it would suit the members to adopt this policy so that it could become binding on the member agencies.

The members agreed.

MR. ARMSTRONG asked Admiral Johnson to present his proposed amendments to the report.

USCIB: 14/100

As a result of Admiral Johnson's proposals and the members' comments thereon, the following amendments to the report were agreed upon:

a. Page 1 - Reverse the order of paragraphs 4 and 5 and re-word each to read as follows: EO 3.3(h)(2) PL 86-36/50 USC 3605

"4. U.S.-French collaboration has become so close as to require, in particular, the improvement of the security of French communications. Such improvement entails an advantage outweighing the value of the [redacted] which would probably be lost thereby.

"5. Because of general French insecurity, the immediate advantages accruing to the security of the U.S. by urging improvement of the security of French Diplomatic traffic are likely to be of limited value."

b. Tab A, subparagraph 1a. - Amend subparagraph to read as follows:

"a. Take steps to improve French security in general and cryptographic security in particular. Undertake improvement of French cryptographic security only after there has been established a secure group in the French Government which would enable the U.S. to pass to the French Government without risk of compromise."

Following approval of the above amendments ADMIRAL STONE invited the attention of the members to Paragraph 8, subparagraph b, and read a proposed amendment. He said that he had talked informally with the British on this point - as a result of which he thought the French could be given technical advice on cryptomachinery improvements, but could not be provided with crypto material, except possibly some one-time pads.

MR. ARMSTRONG asked if the members would agree to accept Admiral Stone's proposed revision of 8b.

All members agreed that this paragraph would be changed to read:

"b. If the provision by the U.S. or U.K. of a cryptographic system for communications proves to be impractical, then use by the French of their own best cryptographic system would be the next most desirable solution."

USCIB: 14/100

ADMIRAL JOHNSON asked if this report should be forwarded to the Secretary of State and the Secretary of Defense for information at this time.

MR. ARMSTRONG said that he thought such forwarding would be automatic.

ADMIRAL STONE then referred to subparagraph 8d. and said that it should include a statement regarding technical assistance by the U. S. and U. K. to the French.

[redacted] in reply to a question, stated that this statement in the report (8d) meant that the French had the technical knowledge to know a good system from a bad one but that they had insufficient money and personnel to exploit their knowledge.

OGA

ADMIRAL STONE expressed his opinion that without U.S.-U.K. technical assistance and advice, the use by the French of their own systems would not necessarily achieve the result we thought desirable.

After a brief discussion the members agreed that subparagraph 8d should be amended to reflect the general thought expressed by the members at this meeting. It was also agreed that the Coordinator would prepare the appropriate wording for this subparagraph.

DECISION: USCIB accepted the report of the Security Committee as contained in USCIB: 14/96, with amendments as indicated in the above discussion. It was agreed that the decision on the appropriate time for forwarding the report to the National Security Council will be deferred for further action by USCIB, but that this report be furnished now to the State and Defense representatives who will be engaged in detailed negotiations with the French on this problem. These negotiators will, at their discretion, forward the report to their superiors.

This item to be dropped from the agenda.

The full report as revised is as follows:

THE POSITION OF THE UNITED STATES REGARDING IMPROVEMENT OF FRENCH DIPLOMATIC CRYPTOGRAPHIC SECURITY

PROBLEM

1. To review French diplomatic cryptographic security, particularly with a view to establishing pertinent U. S. policy and to provide guidance for the U. S. negotiators in their proposed forthcoming discussions with the French on improvement of French over-all security.

DISCUSSION

2. See Tab B.

CONCLUSIONS

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

3. There are no methods whereby the security of French diplomatic cryptographic communications can be improved effectively [redacted]

4. U.S.-French collaboration has become so close as to require, in particular, the improvement of the security of French communications. Such improvement entails an advantage outweighing the [redacted] which would probably be lost thereby.

5. Because of general French insecurity, the immediate advantages accruing to the security of the U. S. by urging improvement of the security of French Diplomatic traffic are likely to be of limited value.

6. Therefore, steps should be taken to improve French diplomatic cryptographic security only as soon as there is established within the French Government a secure group to which the U. S. may pass highly classified information of combined interest without risk of compromise. No steps toward the improvement of French diplomatic cryptographic security should be taken or discussed until this condition has been achieved. However, such steps need not await a total improvement of over-all French security.

7. It is not possible, at present, to determine either (a) the precise approach which should be used to undertake these steps or (b) the degree to which it may be necessary to reveal the evidence of French insecurity derived from the [redacted]

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

8. If and when steps are taken to improve French diplomatic security, the following conditions apply:

a. Provision by the U. S. or U. K. of a cryptographic system for French communications is considered to be the most desirable solution to this problem.

b. If the provision by the U.S. or U.K. of a cryptographic system for communications proves to be impractical, then use by the French of their own best cryptographic system would be the next most desirable solution.

c. Other methods for solving this problem are not satisfactory.

d. It is considered that the U.S. or U.K. should afford the French technical assistance and advice in connection with any method adopted to improve communications security.

RECOMMENDATION

9. That the National Security Council approve the attached Statement of Policy (Tab A).

USCIB: 14/100

TAB A

STATEMENT OF POLICY

on

THE POSITION OF THE UNITED STATES REGARDING IMPROVEMENT OF FRENCH DIPLOMATIC CRYPTOGRAPHIC SECURITY

1. The United States in discussions with the French on the improvement of French security should:

a. Take steps to improve French security in general and cryptographic security in particular. Undertake improvement of French cryptographic security only after there has been established a **secure group in the French Government which** would enable the U. S. to pass to the French Government highly classified information of combined interest without risk of compromise.

b. Avoid placing the question of French diplomatic communications security on the agenda for the first discussion with the French, and on subsequent agenda, until such time as improvement of other security matters had demonstrated that the French have made definite progress toward over-all security.

c. Postpone, on a "No comment" basis, any discussion in the event that this problem is raised by the French prior to being placed on the agenda for discussion.

2. This aspect of the general problem of French over-all security will be coordinated with the U.K. prior to any approach to the French concerning improvement of their diplomatic cryptographic security.

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

3. USCIB is charged with the responsibility:

a. To designate an official to represent USCIB in determining, along with U.S. negotiators, the most advisable approach to be used and the degree to which it may be necessary to reveal [redacted]

b. **To develop with appropriate U.K. authorities a combined policy affecting this problem.**

c. To determine and advise the U.S. negotiators when there have been established within the French Government those conditions which are prerequisite to U.S. efforts toward the improvement of French diplomatic cryptographic security. No such efforts shall be made by the negotiators without the advice and concurrence of the USCIB representative.

TAB B

DISCUSSION

1. The threat to U. S. security which derives from the insecurity of French communications has been a matter of deep concern to the United States for some time past.

a. In August 1948, USCIB considered this problem and submitted a split report for decision by the National Security Council. No action toward the improvement of French cryptographic security was taken at that time.

b. In September 1949, USCIB, on behalf of the U. S. Government, accepted a British proposal that a British cryptographic device be provided to all NATO governments for use as part of the COSMIC system. This device was adopted by NATO.

c. Recently the problem of French cryptographic security has become increasingly critical. As the scope of U.S.-U.K.-French collaboration has been extended, the French Minister of Defense has approached U.S. and U.K. representatives with regard to improvement of over-all French security. Hence a re-study by USCIB of the cryptographic aspects of French security is indicated.

2. Any consideration of French cryptographic security must involve the questions of whether it would be advisable to take action toward the improvement of French communications security practices and procedures, and if so, the nature and scope of corrective measures to this end.

3. Studies conducted by intelligence agencies of the United States indicate that French government departments and agencies are penetrated extensively by the Communists and, therefore, their present over-all security is very poor. It would thus appear that the improvement of cryptographic security at this time, without an accompanying improvement in other security aspects, would have limited value.

[redacted] therefore, corrective measures should be addressed toward either (a) the exclusion of U.S. information from French diplomatic communications or (b) improvement of French diplomatic cryptographic security. Inasmuch as the U.S. cannot completely control French dissemination of U.S. information, it is clear that optimum corrective

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

measures must include an improvement in French diplomatic cryptographic security. Therefore, this study has been directed toward this end.

[redacted]

7. Nevertheless, early steps looking toward this improvement would entail advantage through the development of secure communications practices within the French Government. Good cryptographic security is not a condition which can be imposed all at once. The physical machinery involved might be provided and distributed in a very short time, but the intangible factors, such as training, technical skill (in both use and maintenance), security awareness, and smooth cooperation among widely scattered operating elements, constitute a structure which requires a great deal of time to build.

8. Ultimately the improvement of French cryptographic security may be necessary on all communication links to avoid leaks through retransmission to other offices or lower echelons in poor cryptographic systems, but some advantage will accrue from progressive improvement commencing with specific links carrying important information of combined interest.

9. Assuming that a decision is ultimately made to proceed with the improvement of French cryptographic security, four possible methods exist whereby this improvement of French communications security may be undertaken:

a. The establishment of combined cryptocenters for the reencipherment of all U.S., U.K., and French traffic passing information of a combined interest. This system envisages the initial encipherment of the traffic of each nation in the cryptographic systems of that nation.

b. A requirement on the French that they use their own best cryptographic systems.

c. The provision by another foreign country of a cryptographic system for French communications.

d. The provision by the U. S. or the U. K. of a cryptographic system for French communications.

10. Joint cryptocenters for re-encipherment. Although this method would appear to have the least adverse effect on the [redacted] it seems to be the least desirable of the four methods enumerated above. This method would be too complex and cumbersome for efficient use. It would not be sufficiently expandable to accommodate any large number of French communication links. It is doubtful that this method would be acceptable operationally to the U. S. and the U. K.

11. A requirement that the French employ their own best cryptographic systems. This method would appear to have the greatest adverse effect on the [redacted] Among the adequate French cryptographic systems, only their military cipher devices would appear to meet the needs of extensive, efficient communications.

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

12. Provision by another foreign country of a cryptographic system for French communications. In view of the apparent capacity of the U. S. and U. K. to provide adequate cryptographic equipment under controlled conditions, it appears unnecessary to look elsewhere for this assistance.

13. Provision by the U. S. or the U. K. of a cryptographic system for French communications. Of the four methods enumerated above, this method would appear to be the best. So far as can be foreseen, it would have neither the least nor the greatest adverse effect [redacted] Although this method would involve the use of U. S. cryptographic equipment under conditions which this Government cannot control directly, it is estimated that the risk of compromise to U. S. cryptography is slight. It appears that the U. S. and U. K. have the capacity to provide adequate cryptographic equipment for those French communication links which are expected to carry information of combined interest. It may be noted that a precedent for this method exists in the present NATO agreement whereby a U.K. cipher device has been issued to certain elements of the NATO governments. This precedent, if extended within the French Government, would be most easily extended within other governments if similar problems should arise with other NATO countries in the future.

TOP SECRET ACORN

FINAL

SUBJECT NUMBER

USCIB: 5/269 Item 1 of the Agenda for the Fifty-eighth Meeting of USCIB, held on 8 December 1950.

Subject: Approval of the Minutes of the Fifty-seventh Meeting.

MR. ARMSTRONG asked for comments on the tentative version of the Minutes of the Fifty-seventh Meeting.

GENERAL CANINE invited the attention of the members to the Decision on page 17, and said that he would like to propose that the Decision be changed to read as follows:

> "USCIB accepted the report of the Security Committee as contained in USCIB: 14/96, with amendments as indicated in the above discussion. It was agreed that the decision on the appropriate time for forwarding the report to the National Security Council will be deferred for further action by USCIB, but that this report be furnished now to the State and Defense representatives who will be engaged in detailed negotiations with the French on this problem. These negotiators will, at their discretion, forward the report to their superiors."

The members accepted this proposed change.

MR. ARMSTRONG referred to his statement as contained in the 2nd paragraph on page 17 and said that the idea that he had intended to convey was that forwarding of the report to the Secretary of State and the Secretary of Defense could be considered accomplished, constructively. He added that in view of approval of General Canine's proposal, however, there was no real need to amend his statement.

MR. ARMSTRONG then stated that there were two other actions required by the Security Committee Report, upon which the Board had not made a decision. These were:

Tab E

> (a) The naming of a Board member to serve as a liaison officer for the Board with the designated negotiators on the French problem, and
>
> (b) The designation of a representative to assume coordination responsibility with LSIB (through Brigadier Tiltman) on the development of a US/UK policy with regard to French communications security.

USCIB: 5/269

MR. ARMSTRONG suggested, for the members' consideration, that the USCIB Coordinator be designated to represent the Board in each of the above capacities.

The COORDINATOR expressed his willingness to be the representative of the Board in these matters and the members agreed that he would be so designated.

MR. ARMSTRONG asked for any other comments on the minutes of the Fifty-seventh Meeting.

GENERAL AGEE commented that his Department had previously submitted to the Secretariat several minor changes; however, they had been changes in form rather than substance.

The Secretary stated that these changes had been inserted.

DECISION: The members agreed to accept the minutes of the Fifty-seventh Meeting with the amendments noted above.

(SECRETARY'S NOTE: In view of the above decision this item is dropped from the "Pending Actions" section of the agenda.)

USCIB: 14/112

APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL

8 January 1951

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Security of Foreign Communications.

1. The attached letter on the above subject is forwarded at the direction of the Chairman, USCIB.

2. This subject will be discussed as an item of the agenda for the Fifty-ninth Meeting, 12 January 1951.

H. D. JONES
J. W. PEARSON
Secretariat, USCIB

APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL

USCIB: 14/112

Tab F

TOP SECRET ACORN

London

12th December, 1950

SB/783

Chairman,
United States Communication Intelligence Board.

Subject: THE INSECURITY OF FRENCH DIPLOMATIC CYPHERS

In accordance with the U.S. - British Communication Intelligence Agreement, L.S.I.B. wishes to raise with U.S.C.I.B. the problem of the insecurity of French cyphers as a matter affecting Third Parties to the Agreement (paragraph 5).

2. This problem was the subject of an exchange of views between the American and British Secretaries of State for Foreign Affairs in 1948. At that time Mr. Bevin said that, in view of the gravity of the issues at stake, he thought that the French should be informed with [redacted] and this in spite of objections from his expert advisers. Mr. Marshall, however, replied that the National Security Council was unable to accept the British proposals.

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

3. It is the view of L.S.I.B. that circumstances now exist which require a re-examination of this problem. In the first place, though British cyphers have been, or are in course of being, provided to France and other countries for the transmission of international traffic dealing with Western Union and N.A.T.O. affairs, the security of French telegrams on related or national subjects is still seriously inadequate. Secondly, the trend of international events makes any French cryptographic weakness increasingly inimical to U.S. and British interests. Finally, it is important that the Comint agencies should reach agreement now about the action required so that it may be taken at the first appropriate moment.

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

4. L.S.I.B. is of the opinion that French cypher security can only be adequately improved by the French undertaking a complete reorganisation of their arrangements and accepting outside technical advice. It will be difficult to persuade the French that these radical measures are necessary, and to convince them we may have to inform them [redacted] In giving them this information, we will almost certainly be denying ourselves the [redacted] So great, however, is the importance attached to a real improvement of French cypher security that L.S.I.B. is prepared to accept the [redacted]

5. It is proposed that we should first approach the French at the highest level and inform them:

[redacted]

(c) that, should they not believe this, we are prepared to demonstrate it to their experts provided they will agree:

(i) completely to overhaul their cypher arrangements,

(ii) to accept the appointment of British and/or U.S. experts to assist them.

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

Only when all arrangements for the appointment of our experts were completed would we proceed to the [redacted]

7. L.S.I.B. therefore seeks the concurrence of U.S.C.I.B. to the following proposals:

(a) that there should be agreement in principle that an approach to the French on the lines suggested above should be made at an appropriate time;

(b) that A.F.S.A. and G.C.H.Q. should co-operate in working out the technical details of the action required, both as to what information should be divulged and what cryptographic advice and assistance should be given;

(c) that to effect this collaboration, A.F.S.A. and G.C.H.Q. should independently work out plans which would be brought together at a conference to be held early in 1951;

(d) that, once the combined technical plan has been agreed, further consideration should be given to deciding when, how and by whom the plan should be implemented.

8. In order to save time and in the hope of U.S.C.I.B. agreement to these proposals, the technical research required for 7(c) above has already been set in motion at G.C.H.Q.

/s/ [redacted]
Chairman,
London Signal Intelligence Board.

PL 86-36/50 USC 3605

SB/783