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.

MR. COLLINS said that he had nothing to add to the report, but would be glad to answer any questions.

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.

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.

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:

"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]

E.O. 3.3(h)(2)
PL 86-36/50 USC 3605

"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."

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.

MR. COLLINS, 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.

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

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].

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 [redacted]

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.

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 [redacted]

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

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.

USCIB: 14/100

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]

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

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.

USCIB: 14/100

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 [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 [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 [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.