USCIB: 23/49

22 April 1953

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Proposed U.K./U.S. Conference on the Security of Diplomatic Ciphers Employed by France and Other NATO Countries.

Reference: USCIB 23/48 dated 31 March 1953.

Vote sheet replies to the reference indicate the approval of all members. Accordingly, the draft memorandum contained in enclosure 2 with the reference has been forwarded to the Chairman, LSIB.

H. D. JONES
Acting Executive Secretary, USCIB

USCIB: 23/49

24

31 March 1953

~~TOP SECRET CANOE - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Proposed U.K./U.S. Conference on the Security of Diplomatic Ciphers Employed by France and other NATO Countries.

1. There is attached a copy of a communication from the Chairman of the London Signal Intelligence Board proposing a conference, in the near future, between representatives of USCIB and LSIB on the following questions:

a. To review, in light of recent developments, the proposed tactics of the approach to the French regarding insecurity of their diplomatic ciphers.

b. To consider strategy on the wider question of the insecurity of the diplomatic ciphers of other NATO nations.

In addition, the Chairman, LSIB, has proposed that a related subject, viz, the security of the ciphers used by the armed forces of France and other NATO countries, be considered provided such would not hold up action on the matters referred to in (a) and (b) above.

2. The Chairman, USCIB, has expressed his opinion that the facts cited in the attached memorandum from the Chairman of LSIB, plus other facts on this subject which have, from time to time, been brought to the attention of the Members of USCIB, justify having the proposed conference in the near future.

3. There is appended as Enclosure 2, a draft reply to the Chairman, LSIB, for signature by the Chairman, USCIB. It is requested that your concurrence or comments with reference to this reply be returned to the Secretary on the attached vote sheet at your early convenience, preferably not later than Tuesday, 7 April 1953.

H. D. JONES
Acting Executive Secretary, USCIB

Enclosures - 2
1. DGC/3242 dtd 26 Feb 53.
2. Draft Reply to DGC/3242 from Chairman, USCIB.

USCIB: 23/48

DGC/3242

26th February, 1953.

Chairman,
United States Communications Intelligence Board.

---

1. One of the conclusions of the U.K. - U.S. Conference on the security of French Communications held at Washington in May 1951 was that "the urgency for improving the security of French diplomatic communications" was "such that a programme to this end should be undertaken as soon as possible".* It was also recommended, however, that any approach to the French M.F.A. should be deferred pending consideration of the report of the Tripartite Group at that time studying the internal security of the French Government.ƒ There must be good evidence, before the initial approach was made, that French authorities having access to M.F.A. communications handled on a classified basis by the U.K. or U.S. Government "have the intent and capability to establish arrangements to protect this information", and that these arrangements should be "sufficient, in the agreed opinion of the U.K. and the U.S. Governments, to warrant making an initial approach".**

2. In December 1951 Chairman L.S.I.B. informed Chairman U.S.C.I.B.‡‡ that L.S.I.B. had examined the report of the Tripartite Group and had concluded that the French intent and capability to establish security arrangements were sufficient to warrant the U.S. and the U.K. making an initial approach to them about their communications security.

3. In reply[x] Chairman U.S.C.I.B. stated that the report of the Tripartite Group on general security did not in itself represent an improvement in French security, and that it was U.S.C.I.B.'s understanding that an approach to the French M.F.A. could not be made until the report had been approved by each of the participating

* Para. 3(1) of Conference report

ƒ Para. 3(k) of Conference report

** Conference report, para. 47(a) of Enclosure 'B'

‡‡ LSIB/244/51

x Dated 24th January, 1952.

Enclosure 1 with USCIB 23/48 dated 31 March 1953.

countries and the French Government had undertaken definite implementing action on the basis of its approval. Following these developments U.S.C.I.B. would, as previously agreed, be prepared to discuss the means for approaching the French M.F.A. along the general lines proposed by L.S.I.B.

4. It is now understood by L.S.I.B. that, in spite of reservations about Civil Ministries, both the U.S. and U.K. delegations to the recent conference of the Tripartite Security Working Group have agreed that positive steps have been taken by the French to put into effect the principles and standards laid down in the 1951 Tripartite report, and L.S.I.B. feels that U.S.C.I.B's principal objection to an early approach to the French is therefore less valid.

5. There have been two other developments since 1951 which affect the situation:

[redacted]

(b) During 1952 there has been a marked improvement in the behaviour of the French on cypher security matters. By and large NATO security rules in this connection have been strictly observed, [redacted]

6. L.S.I.B. considers that the developments outlined in paragraphs 4 and 5(a) and (b) above reflect an improvement in French

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

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

security awareness and in French security itself, and that the risks involved in the proposed approach to the French M.F.A. in 1951 are now much reduced. There is still an urgent need for such an approach, however, both on account of the continuing (though less serious) cypher security weakness of the French M.F.A. itself, and because there is a strong case for putting French cyphers right before proceeding (as the French themselves wish to proceed) to those of other NATO nations.

7. L.S.I.B. feels, however, that it might be desirable for U.S.C.I.B. and L.S.I.B., in the light of recent developments, to review the proposed tactics of the approach to the French on their diplomatic cyphers, and at the same time to consider strategy on the wider question of the diplomatic cyphers of other NATO nations. A further conference of U.S.C.I.B. and L.S.I.B. representatives appears the only satisfactory method of conducting an adequate survey of the current position. A related subject that might appropriately be considered at a conference of U.S.C.I.B. and L.S.I.B. representatives - provided it does not hold up action on the diplomatic cyphers - is the security of the cyphers used by the armed forces of France and other NATO countries. L.S.I.B. feels that at the present time valuable data on NATO forces may be available to the Russians from the exploitation of the cyphers, and that it would be essential to stop such a leak before the outbreak of any war between NATO powers and the Soviet bloc.

8. L.S.I.B. therefore urges that a conference on the above questions between representatives of the two Boards should be convened as early as possible, either in London or in Washington. While L.S.I.B. would like an opportunity to welcome U.S. representatives to London, it would be happy to comply if for any reason U.S.C.I.B. preferred to hold the conference in Washington.

(Signed)

London Signal Intelligence Board

DRAFT

TOP SECRET CANOE - SECURITY INFORMATION

MEMORANDUM FOR THE CHAIRMAN, LONDON SIGNAL INTELLIGENCE BOARD:

Subject: Proposed U.K./U.S. Conference on the Security of Diplomatic Ciphers Employed by France and other NATO Countries.

Reference: DGC/3242 dated 26 February 1953.

1. The proposals contained in the reference have been considered by USCIB members who agree that circumstances justify early U.S.-U.K. discussions to review the proposed approach to the French on their diplomatic ciphers, and to consider what action should be taken, if any, on the wider question of the diplomatic ciphers of other NATO nations.

2. It is also the opinion of our Board that further discussions on the security of the cipher systems used by the armed forces of France and other NATO countries may be worthwhile, with the understanding that the question of diplomatic cipher systems would receive initial attention by the conference.

3. USCIB members would be most pleased to have the U.K. representatives visit Washington for these discussions, and would welcome your suggestion of a suitable date for the opening of the conference. From our viewpoint any date subsequent to the middle of May would be acceptable.

(Draft)
ALLEN W. DULLES
Chairman, United States
Communications Intelligence Board

Enclosure 2 with USCIB 23/48 dtd 31 March 1953.