~~TOP SECRET~~

7

USCIB: 14/185

27 December 1951

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: French Communication Security.

1. The attached letter on the above subject is forwarded for information, with a view to possible discussion at the 73rd Meeting of USCIB.

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

Inclosure - 1
LSIB/244/51 dated 10th December 1951.

USCIB: 14/185

~~TOP SECRET~~

London

10th December, 1951.

LSIB/244/51

Chairman,
United States Communications Intelligence Board.

With reference to your memorandum UC 000227 dated 22nd June 1951, the London Signal Intelligence Board notes that the United States Communications Intelligence Board has approved the report of the U.S./U.K. Conference on the Security of French Communications, but observes that it has not yet been advised of the decision of the National Security Council.

Not yet approved by UK/France - per Denvir 16 Jan 52

2. In paragraph 3(k) of the Conference report, it was concluded that any approach to the French Ministry of Foreign Affairs should be deferred pending consideration of the report of the Tripartite Group. L.S.I.B. has now examined the Tripartite Group's report and concludes that the French intent and capability to establish security arrangements are sufficient to warrant the U.S. and the U.K. making an initial approach to them about their communication security.

3. L.S.I.B. proposes that the U.S. and U.K. Ambassadors should be briefed according to the document attached as Appendix 'A' and that the approach should be made at the first opportunity. L.S.I.B. also proposes that, in order to preserve an appearance of non-cooperation between the U.K. and the U.S. [redacted] the U.K. Ambassador should make the first approach, to be followed a few days later by that of the U.S. Ambassador.

4. L.S.I.B. further proposes that the U.S.C.I.B. and L.S.I.B. nominees who according to paragraph 55 of the Conference Report, are to be available in Paris to take part as required in the initial discussions with the French should meet in London a day or two in advance in order to coordinate final details. For this purpose L.S.I.B. will nominate a senior representative and an expert from G.C.H.Q. In anticipation of U.S.C.I.B. concurrence to this proposal, a list of examples of French insecurity suitable for demonstration is in course of preparation at G.C.H.Q. and would be ready for the preliminary meeting between the U.S.C.I.B. and L.S.I.B. nominees.

5. U.K. authorities can provide, in two months time, 8 CCM machines to be offered to the French.

6. L.S.I.B. would welcome U.S.C.I.B.'s comments on these proposals at its earliest convenience.

[redacted]
Chairman
London Signal Intelligence Board

Inclosure with USCIB 23/43 dated 27 December 1951.

LSIB/244/51

Appendix 'A'

BRIEF TO U.S. AND U.K. AMBASSADORS IN PARIS

The U.S. and U.K. Governments, having been convinced that the cypher communications of the French MFA are so thoroughly insecure as to be inimical to the interests of the Western powers, have decided to approach the French Government on the matter. They regard the security of French diplomatic communications as of the greatest importance and are therefore prepared to offer material help towards improving them.

[redacted]

3. The U.S. and U.K. Governments therefore think it reasonable to assume that French diplomatic communications are an invaluable source of intelligence to Russia on Western diplomacy and strategy, indeed that they may well be her most prolific, most speedy and most reliable source of all. They regard it as imperative that Russia should be deprived of this source, not only so that she will be denied the intelligence now accessible to her from it, but also so that officials of the U.S. and U.K. Governments may more freely discuss important matters of common concern with officials of the French Government.

4. So bad are the cypher systems and communication practices of the French MFA that, in the opinion of the U.S. and U.K. Governments, the situation can only be satisfactorily improved by a drastic and expensive reorganisation of the Cypher Service of that Ministry and the appropriate replacement of its systems and practices. In order to ensure a realisation by the French MFA that such a drastic overhaul is necessary, it is essential that the situation should be brought to notice in a manner so dramatic and convincing as to shock the Ministry into taking speedy and effective action.

5. The U.S. and U.K. Governments have therefore decided to instruct their Ambassadors in Paris to inform the Secretary - General of the French MFA, M. Alexander Parodi, that French diplomatic cyphers are completely insecure, [redacted] and that, as remedying this state of affairs requires drastic and expensive action, the U.S. and U.K. Governments are willing to help in instituting corrective measures provided he will give assurances that his Ministry will:

(a) undertake an energetic programme for reorganisation of its Cypher Service and appropriate replacement of its present systems and practices;

(b) accept without qualification and promulgate U.K./U.S. essential standards of security in each phase and aspect of the programme;

(c) accept direct U.K./U.S. participation in executing the programme, including participation on a working level by representatives qualified in the field of general security as well as all aspects of communication security.

/6. Should

LSIB/244/51

Appendix 'A'

[redacted]

7. If M. Parodi is willing to accept these proposals, the U.S. and U.K. Governments are for their part willing to provide as a minimum, on long-term loan, sufficient Combined Cypher Machines (CCM) to equip about 30 of the most important diplomatic posts with two machines each, a quarter to a third of them at once and the remainder phased in consonance with NATO requirements. (This machine has already been accepted by the French Government for high-level NATO communications.) For those posts which cannot immediately be equipped with CCM Machines, and as a standby for those which can, the U.S. and U.K. Governments propose one-time pads and are prepared to advise on and assist in their construction. M. Parodi can be assured that, as the French would be producing their own settings for the Cypher Machines and their own one-time pads, their telegrams would not be readable by the U.S. and British Governments.

8. The U.S. and U.K. Ambassadors in Paris should be aware that two of the problems which their Governments have had to face in arriving at these conclusions have been

[redacted]

/report

LSIB/244/51

Appendix 'A'