

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

Subject: LSIB Proposals Re French Security.

Reference: Letter from Chairman, LSIB to Chairman, USCIB, on above subject, 12 December 1950.

Enclosures: A. Report, etc.
B. Draft of letter to Chairman, LSIB.

1. With regard to paragraph 7(c) of the reference, which was considered at the Fifty-ninth Meeting of USCIB, the attached report (Enclosure A) has been prepared, at the direction of DIRAFSA, to serve as a U. S. position in discussions with British representatives on or about 1 April 1951.

2. It is requested that the attached report be considered in connection with Item 5 of the agenda for the Sixtieth USCIB Meeting, to be held on 9 February 1951.

3. a. It should be noted that the attached study is responsive to the enclosure USCIB 14/112 and is therefore confined to the French diplomatic cipher security problem. However, as pointed out in Par. 1 of the Enclosure "B" to USCIB 14/118, it is clear that cipher insecurity permeates the entire area of French communications, including military, naval, and probably air communications as well as diplomatic. Therefore, even though the U. S. and the U. K. have already provided the French military authorities with secure cryptographic machines ^{and systems} (TYPEX) and are now considering providing them also

~~TOP SECRET~~

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

with the CCM for the transmission of international traffic dealing with Western Union and NATO affairs, the security of wholly intra-French military communications on related or purely national subjects will remain seriously inadequate and thus will jeopardize the security of NATO, purely U. S., purely U. K., and U.S.-U.K. communications. Hence, it^{is} clearly insufficient to overhaul French diplomatic cryptography, and the security problem must be resolved in respect to French cryptographic systems in all areas, military, naval, air, etc., as well as in the diplomatic area.

b. It is therefore recommended that the agenda for any discussions with the British on the subject of French diplomatic cipher insecurity be broadened to include all French cryptographic communications and that a proposal to this effect be made to the chairman of LSIB. Enclosure B is a draft of a letter embodying such a proposal.

EARL E. STONE
Rear Admiral, U.S. Navy
USCIB Coordinator

~~TOP SECRET~~

~~TOP SECRET~~

D R A F T

Chairman,
London Signal Intelligence Board

Subject: THE INSECURITY OF FRENCH DIPLOMATIC CIPHERS

In accordance with Paragraph 7(c) of SB/783, the plan which AFSA has worked out is embodied in Enclosure A hereto and is forwarded in advance of the conference to be held early in 1951, as proposed in the paragraph of reference.

2. a. It should be noted that Enclosure A is responsive to SB/783 and is therefore confined to the French diplomatic cipher security problem. However, as pointed out in Paragraph 1 of the Enclosure "B" to Enclosure A, it is clear that cipher insecurity permeates the entire area of French communications, including military, naval, and probably air communications as well as diplomatic. Therefore, even though the U. S. and the U. K. have already provided the French military authorities with secure cryptographic machines and systems (TYPEX) and are now considering providing them also with the CCM for the transmission of international traffic dealing with Western Union and NATO affairs, the security of wholly intra-French military communications on related or purely national subjects will remain seriously inadequate and thus will jeopardize the security of NATO, purely U. S., purely U. K., and U. S.-U. K. communications. Hence, it is clearly insufficient to overhaul French diplomatic cryptography, and the security problem must be resolved in respect to French cryptographic systems in all areas, military, naval, air, etc., as well as in the diplomatic area.

~~TOP SECRET~~

D R A F T

~~TOP SECRET~~

3. USCIB therefore seeks the concurrence of LSIB to expand the scope of the conference to be held early in 1951 to include discussions regarding action required to improve the security of French governmental communications in all areas.

4. The plan which AFSA has worked out as regards the improvement in French diplomatic communications (Enclosure A) is readily susceptible of application to French military, naval, and air communications of the highest echelons down to and including those of headquarters of Division. Should the discussions at the forthcoming conference extend into the field of tactical communications of formations below those equivalent to division headquarters, it is probable that the recommendations which would be made to the French authorities concerned would have to be examined in the light of what disclosures would be required

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

~~TOP SECRET~~