~~TOP SECRET~~

USCIB: 14/119

7 February 1951.

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: LSIB Proposals Re French Security.

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

Enclosures:
A. Report by the Coordinator to USCIB on above subject.
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 and plan in discussions with British representatives on or about 1 April 1951.

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

3. a. It should be noted that the attached report is responsive to the Enclosure to USCIB: 14/112 and is therefore confined to the French diplomatic cipher security problem. However, as pointed out in paragraph 1 of Enclosure "B" to USCIB: 14/119, it is clear that cipher insecurity permeates the entire area of French communications, including military, as well as diplomatic. Therefore, even though the U. S. and the U. K. provide the French military authorities with secure cryptographic machines and systems 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 may jeopardize the security of Western Union, NATO, purely U. S., purely U. K., and U. S. - U. K. communications.

b. It is therefore recommended that the agenda for the proposed discussions with the British on the subject of French diplomatic cipher insecurity be broadened to include the question of improving all French cryptographic communications, and that a

USCIB: 14/119

CODE WORD MATERIAL

~~TOP SECRET~~

USCIB: 14/119

7 February 1951

Subject: LSIB Proposals Re French Security.

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

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

~~TOP SECRET~~

5 February 1951

MEMORANDUM FOR THE DIRECTOR, AFSA:

Subject: Cooperation with GCHQ in Regard to Action Required on Insecurity of French Communications.

Reference: Memorandum for AFSA-OOT, above subject, 22 January 1951.

Enclosure: Draft of Report by the Coordinator to USCIB on above subject.

1. The report called for in paragraph 3d of the reference is forwarded herewith.

2. In the course of its study of the problem, the Ad Hoc Committee gave due consideration to the points raised in paragraph 4 of the reference and submits, with regard thereto, the following comments:

a. (Reference subparagraph 4a.) After consideration of the technical aspects of the communications security practices of other governments with which the U.S. is now allied in NATO, the Committee agreed that the problem, as it concerns the French, was unique and deserving of individual and prompt attention.

b. (Reference subparagraph 4c.) The Committee considered the USCIB decisions to date on this matter, and concluded that they were, and still are, sound from a technical standpoint. Further, it was agreed that the USCIB position, in agreeing to proceed in an effort to overhaul French security through discussions with the British, represents the most logical approach to a solution of the problem. The Committee is of the opinion that positive action is indicated under the circumstances and that the action recommended in the Enclosure is suitable in the premises.

William F. Friedman

W. F. FRIEDMAN
Chairman,
Ad Hoc Committee

~~TOP SECRET~~

~~TOP SECRET~~

5 February 1951

MEMORANDUM FOR THE DIRECTOR, AFSA:

Subject: Cooperation with GCHQ in Regard to Action Required on Insecurity of French Communications.

Reference: Memorandum for AFSA-OOT, above subject, 22 January 1951.

Enclosure: Draft of Report by the Coordinator to USCIB on above subject.

1. The report called for in paragraph 3d of the reference is forwarded herewith.

2. In the course of its study of the problem, the Ad Hoc Committee gave due consideration to the points raised in paragraph 4 of the reference and submits, with regard thereto, the following comments:

a. (Reference subparagraph 4a.) After consideration of the technical aspects of the communications security practices of other governments with which the U.S. is now allied in NATO, the Committee agreed that the problem, as it concerns the French, was unique and deserving of individual and prompt attention.

b. (Reference subparagraph 4c.) The Committee considered the USCIB decisions to date on this matter, and concluded that they were, and still are, sound from a technical standpoint. Further, it was agreed that the USCIB position, in agreeing to proceed in an effort to overhaul French security through discussions with the British, represents the most logical approach to a solution of the problem. The Committee is of the opinion that positive action is indicated under the circumstances and that the action recommended in the Enclosure is suitable in the premises.

William F. Friedman

W. F. FRIEDMAN
Chairman,
Ad Hoc Committee

~~TOP SECRET~~

~~TOP SECRET ACORN~~

REPORT BY THE COORDINATOR,
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

to the

UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

on

COOPERATION WITH GCHQ IN REGARD TO
IMPROVING THE SECURITY OF FRENCH COMMUNICATIONS
Reference: USCIB 14/112 of 8 January 1951

THE PROBLEM

1. In preparation for a BRUSA conference on the subject, to examine present French cryptographic procedures, and to formulate a U. S. plan for improvement of the security thereof.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B."

CONCLUSIONS

3. It is concluded that:

[redacted]

[redacted]

c. This situation can be corrected only by a complete overhaul and replacement of the present insecure cryptographic systems by secure systems.

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

d. The importance of denying this source of COMINT to Russia is such that it is in the interest of the United States [redacted] to provide, at least in part, the cryptographic devices essential to security.

e. Negotiations with the French should be conducted in such a manner that [redacted]

f. Negotiations with the French should, if practicable, be

conducted entirely by the British [redacted]

g. Negotiations should not be instituted prior to the formation of a secure group within the French Government.

RECOMMENDATIONS

4. It is recommended that:

a. USCIB note and approve the above conclusions.

b. Approve the cryptographic plan for French diplomatic communications contained in Enclosure "A."

ENCLOSURE "A"

PLAN FOR IMPROVING THE CRYPTOGRAPHIC SECURITY OF FRENCH DIPLOMATIC COMMUNICATIONS

1. The proposal presented herein for ensuring the security of French diplomatic communications considers that the various French diplomatic posts should be subdivided into three categories:

a. Category I: A small group of locations which handle the most critical information, such as Paris, London, and Washington.

b. Category II: All capitals not included in a. plus a selected group of important cities whose communications frequently include information of considerable intelligence value.

c. Category III: All other diplomatic posts.

2. The systems recommended, respectively, for the three categories listed above are:

a. For Category I: The Combined Cipher Machine with Simplex keys. The word Simplex is used to mean a procedure whereby each message has its own rotor arrangement and alignment provided by means of a special key list. The lists are prepared for point-to-point use so that each station can read only those messages specifically addressed to it. For the exceptional cases of multiple-address messages, a multiple holder key list is provided. A one-time pad system should be provided as an emergency stand-by in this category.

b. For Category II: The M-209 with special settings used to encipher messages set up in a literal code. The code book used should be a new book specically designed for this sole purpose. Each holder in this category should be provided with three distinct systems; one for use solely with Paris, one for use laterally on a limited regional basis, and one for use laterally on a world wide basis.

c. For Category III: Present French systems would continue to be used.

3. The stations in each category will be included as holders in the categories below them.

4. The merit of these proposals is the provision of a fairly high degree of security for French diplomatic communications, together with a minimum disclosure to the French of systems and ideas with which they are not already familiar. For the transmission of international traffic dealing with Western Union and NATO affairs, they have been provided with TYPEX machines and they are presently using a Simplex procedure with these machines in the highest echelons of NATO; the Combined Cipher Machine is also being offered to them, as well as to other NATO signatories, for NATO communications; French Army, Navy, and Air Force personnel are familiar with and have some copies of the M-209, so that they have experience in the preparation of M-209 settings and can instruct French diplomatic officials in the use of the M-209.

5. The localization introduced by Simplex procedures in Category I and by special or area settings in Category II has a double advantage. First, it increases the cryptosecurity generally; and secondly, if there should be an instance of penetration by the Russians which grants access to cryptographic information, the dangers resulting from such penetration are confine to the single cryptonet involved. This results in minimizing the consequent loss of information.

6. Adequate training in the new systems will be greatly simplified as a result of the already-existing familiarity with them.

7. The establishment of appropriate communications security procedures will be facilitated by the issue of JANAP 122(B) (the U.S. Joint Manual on Communications Security), which is presently under consideration for use in connection with NATO cryptographic systems.

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

[redacted]

2. From an over-all consideration it is concluded that if the French diplomatic cryptographic systems are to be improved it would be necessary to:

a. Replace the current French diplomatic systems with secure systems for use in all important diplomatic posts.

b. Provide adequate training in the new systems for French cryptographic personnel.

c. Establish appropriate communications security procedures in the French Foreign Office.

d. Maintain careful technical supervision over the French diplomatic communications.

3. In regard to the current French diplomatic systems, it is concluded that observed French cryptographic practices in system design and distribution provide direct evidence that the present cryptographic organization does not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed. It is also concluded that, except as regards infrequently used one-time pad systems, none of the French diplomatic cryptographic systems possesses sufficient inherent security to permit its improvement to a point where it may be considered acceptable. It is therefore necessary to discard the current systems and replace them with other systems based on better cryptographic principles.

4. [redacted] show a lack of appreciation by the French Foreign Office of the importance of even the elementary principles of communications security. Therefore, able technical assistance from outside the French diplomatic cryptographic service is deemed essential for the success of any communication security program.

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

5. In view of the foregoing, it is concluded that a complete "housecleaning" of the French diplomatic cryptographic service would be necessary. This would involve not only informing the French that their present diplomatic systems are considered insecure but also establishing a basis on which the French would be provided with appropriate technical assistance to enable them to reorganize their cryptographic service to insure secure handling of communications.

[redacted]

necessary to provide the French [redacted]

7. The British in the past have had many contacts with the French cryptologists. It appears advantageous that, if the French are approached on this matter, it be done unilaterally and initially by the British. Such a course of action would present additional advantages in that (a) it would be unnecessary to disclose the fact or [redacted] and (b) it would limit the number of technicians who would contact the French, and consequently become known to them.

8. The possibility of Russian penetration of the French foreign service cannot be ignored. Penetration may be either complete or partial, and may extend into either the sources of information or into the cryptographic service. Complete penetration of either type would make totally ineffective any plan for improving cryptographic security. [redacted] without denying information to the Russians. Therefore, before any steps are taken, there must be reasonable assurance that there exist secure groups in the French Foreign Office and the office which controls the cryptologic service. In addition to this, the plan proposed should provide the maximum possible protection against the effects of partial penetration of either type.

9. One-time pad systems would provide the necessary security but it does not appear feasible to recommend such a solution. The cumbersome operational characteristics of such systems and the labor required to prepare the pads in the required quantity would probably make a proposal of this kind unacceptable to the French. Likewise, the provision of modern secure machine systems in the required numbers would

TOP SECRET ACORN

probably be beyond the physical capacity of the French government at this time. Nor can the United States undertake the supplying of materials on the scale which would be required.

10. The plan proposed in Enclosure "A" represents a reasonable compromise which will provide adequate cryptographic security for the highest level diplomatic communications and a degree of security for those of lower level which will, if properly used, effectively prevent the production of a significant amount of communication intelligence therefrom.

D R A F T

MEMORANDUM FOR THE CHAIRMAN, LSIB:

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,

Enclosure "B"

naval, air, etc., as well as in the diplomatic area.

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

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

[redacted]

FOR THE UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD:

W. PARK ARMSTRONG, Jr.
Chairman