REF ID:A522818

~~TOP SECRET~~

COPY

USCIB: 14/58

20 July 1949

MEMORANDUM FOR MEMBERS OF USCIB:

Subject: Proposed Measures for Improving the Cipher Security of Western Union Communications.

Enclosure: (A) USCIB SECCOM Special Report No. 7-49.
(B) Chairman, LSIB Memorandum dated 30 June 1949, SB/578.

1. At the request of the Chairman, USCIB, the memorandum from the Chairman, LSIB, "Western Union Organization, Security of Communications" (Enclosure (B)) was referred to the Security Committee for study. The recommendations of that Committee with respect to the LSIB proposals are forwarded herewith as SECCOM Special Report No. 7-49 (Enclosure (A)). This report will be considered under Item 2 of the agenda for the Forty-third meeting of the Board.

/s/P. J. Karl
for H. D. JONES
P. J. KARL
Secretariat, USCIB.

USCIB: 14/58

~~TOP SECRET~~

Declassified and approved for release by NSA on 06-11-2014 pursuant to E.O. 13526

REF ID:A522818

Copy

~~TOP SECRET~~ ~~TOP SECRET~~ 20 July 1949

USCIB SECURITY COMMITTEE
SPECIAL REPORT NO. 7-49.
(to USCIB direct)

REPORT ON PROPOSED MEASURES FOR IMPROVING THE CIPHER SECURITY OF WESTERN UNION COMMUNICATIONS

THE PROBLEM

1. To study the memorandum of 30 June from the Chairman, LSIB, to the Chairman, USCIB, and to make recommendations thereon to USCIB.

FACTS BEARING ON THE PROBLEM

2. USCIB: 14/57 of 18 July 1949 conveys this problem to the Committee.

CONCLUSIONS AND RECOMMENDATIONS

3. The Committee presents the enclosed draft of a memorandum from the Chairman, USCIB, to the Chairman, LSIB, and recommends that this memorandum be transmitted in reply to LSIB's memorandum of 30 June. All pertinent considerations and arguments, as the Committee developed them during its study of the problem, are set forth or implied in this draft.

COORDINATION

4. No coordination of this matter with other Committees or authorities has been deemed necessary.

/s/E.S.L. GOODWIN
E.S.L. GOODWIN
Captain, U. S. Navy
Chairman, SECCOM.

Enclosure: Proposed memorandum for the Chairman, LSIB, from the Chairman, USCIB.
SECCOM draft, 19 July 1949.

SECCOM Item No. 54 ~~TOP SECRET~~

REF ID:A522818

~~TOP SECRET~~

SECCOM draft
19 July 1949

~~TOP SECRET~~

COPY

Memorandum for the Chairman, LSIB.

Subject: Cipher security for Western Union communications.

Reference: Memorandum of 30 June 1949 from the Chairman, LSIB, to the Chairman, USCIB, with enclosure (memorandum will hereinafter be referred to as "the Chairman's memorandum" and enclosure as "the Chairman's enclosure".)

1. The reference has been read with interest. It obviously represents the climax of a most involved and difficult study, and the solution which it presents is patently a compromise among violently antagonistic viewpoints.

2. USCIB, acting within the limits of its charter, must be governed in this principally by considerations of the affects of the alternatives on U.S. Communications Intelligence. From this narrow standpoint, any basic improvement of Western Union communication security will be detrimental, either through direct loss of intelligence (consider paragraph 3 of the Chairman's memorandum and possible miscarriages of the entire LSIB proposal) or through indirect loss of intelligence through resultant general European improvement in communication-security consciousness and knowledge. In this latter connection USCIB notes that any improvement of the cipher security of Western Union nations may eventually involve an extension to that of Atlantic Pact nations. USCIB, therefore, while fully concurring in the aeguments presented in paragraph 7 of the Chairman's memorandum, and while recognizing the possibility that considerations of security may override those of intelligence, is constrained to express only qualified approval of the proposed course of action, subject to certain reservations, hereinafter presented.

3. USCIB considers that the proposal of the reference is completely acceptable as a basis for planning for the situation contemplated in paragraphs 6 and 7 of the Chairman's enclosure (that is, the situation attendant upon a state of war or conditions approaching a state of war). USCIB, however, considers that there should be no immediate implementation of

Enclosure with USCIB SECCOM Special Report No. 7-49.

~~TOP SECRET~~

REF ID:A522818

~~TOP SECRET~~

COPY

Subject: Cipher security for Western Union communications.

---

the plan except such minimum measures as may be necessary to permit LSIB to insure the adoption of its proposal, the maximum such, from the USCIB standpoint, being as follows:

(a) Present the Typex Mark II to the Western Union nations as the proposed combined cipher machine for future emergency.

(b) Do not deliver copies of the Typex Mark II to any other nation, but inform the Western Union nations that Typex Mark II will be demonstrated, in London, to any cryptanalysts and cryptographers whom they choose to send to London for a thorough and unlimited study of the machine, the proposed method of its use, and the details of its routine operation.

(c) Contingent on the other W.U. nations' acceptance of the proposal, accumulate, in U.K., the reserve of machines, instructions, and key lists required for the condition contemplated in paragraphs 6 and 7 of the Chairman's enclosure, and give to appropriate representatives of the W.U. nations full knowledge of and access to this accumulation.

4. In presenting the foregoing, USCIB recognizes that the course of action which it recommends fails to take account of the requirements expressed in paragraph 1 of the Chairman's memorandum and the first sentence of paragraph 8 of the Chairman's enclosure (that is, the immediate need for cipher security for the rapid exchange of W.U. communications among the W.U. capitals and high command). USCIB recommends, therefore, that this requirement be met by the proposal of super-encipherment presented informally by signal by the Senior British Liaison Officer as a result of his membership in an ad hoc committee of USCIB which met on 26 August 1948. This proposal, for official record, is reiterated below:

That the U.S. and Great Britain agree upon and provide a common system for the super-encipherment of all messages of a critical nature; that the use of this system be confined to common

REF ID:A522818

SECCOM draft
19 July 1949

COPY

Subject: Cipher security for Western Union communications.

cryptocenters at critical locations, the centers to be manned by personnel of any Western Union nations; that agreement of the Western Union nations be obtained to pass critical information only between points served by these cryptocenters; that all powers reserve the right to cryptograph such messages in their own systems prior to delivery to the common cryptocenter.

That the common means of super-encipherment preferably consist of a one-time tape system capable of the most rapid handling of traffic.

5. USCIB recognizes, further, that its present recommendations do not meet the needs implied in paragraph 4, the second sentence of paragraph 8, and the second point in paragraph 10 of the Chairman's enclosure, but is constrained to state that these considerations are beyond its cognizance. USCIB hopes, however, that the proposals described in paragraph 3 of the Chairman's memorandum (which would tend to be more detrimental to USCIB's narrow interests than any of the more likely developments from LSIB's proposal) can be forestalled by action which will be in accord both with LSIB's proposals and its own demurs, and requests that it be kept informed of pertinent developments.

Chairman USCIB