II J 1/7
II K 2/2
13/

WASHINGTON 25, D. C.

UC # 000321

27 Aug 1952

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE CHAIRMAN, USCIB:

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

Subject: Statement of U.S. Policy.

1. At the USCIB Meeting on 18 July 1952, in discussing the proposal

[redacted]

sources of considerable value.

2. In commenting upon my remarks you referred to the decision of the National Security Council (NSC) in the case of [redacted] Communication security, and stated that a policy has long been established on this subject, the only question before the Board now being how to apply the policy in each specific case.

3. However, since a formal statement of U.S. policy on this question does not appear to exist in the records of USCIB, and since the matter is of vital importance in national defense, I suggest the advisability of obtaining NSC approval of the statement set forth in Inclosure 1.

4. At an AFSAC Meeting on 20 June 1952 the Report of the U.S./U.K. COMSEC Conference mentioned in paragraph 1 above was discussed. One of the recommendations of the conference is to release to NATO governments a number of high-security cryptographic machines. Before giving its approval to the report, which is to be forwarded to the Joint Chiefs of Staff, and because of the [redacted] As Chairman of AFSAC it is incumbent upon me to proceed with the execution of the AFSAC decision. However, if NSC approval of Inclosure 1 is obtained, it will obviously be unnecessary to take the step proposed by AFSAC and I will be in a position to recommend recision of the AFSAC decision to bring the question before NSC via USCIB.

UC # 000321

27 Aug 1952

~~TOP SECRET - SECURITY INFORMATION~~

Subject: Statement of U.S. Policy.

5. With reference to paragraph 4 of Inclosure 1, this paragraph is deemed desirable in the statement of policy in view of the international discussions which usually precede agreement upon cryptographic systems to be employed in the situations and for the purposes indicated therein.

6. A brief history of the subject may be of interest in this connection and is attached as Inclosure 2.

/s/ Ralph J. Canine
RALPH J. CANINE
Major General, US Army
Chairman, Armed Forces Security Agency Council
and
USCIB Coordinator

Inclosures - 2
1. U.S. Policy on Communications Security of Foreign Governments with which the U.S. is Allied Militarily.
2. Brief History of the Problem - COMSEC versus COMINT.

TOP SECRET

TOP SECRET - SECURITY INFORMATION

UNITED STATES POLICY ON COMMUNICATIONS SECURITY OF FOREIGN GOVERNMENTS WITH WHICH THE UNITED STATES IS ALLIED MILITARILY

1. When it is evident that classified information of U.S. origin, or classified information which pertains to mutual defense plans between or among the U.S. and other governments is encrypted in insecure cryptographic systems used by the other governments and as a consequence endangers the U.S. National Security, the U.S. may initiate such action as is appropriate to cause improvement to be made in the communication security of those other governments, even though the [redacted] detrimental to the security of the U.S. and its allies if read by a potential enemy. If the communications [redacted] methods and the government employing the particular cryptographic systems used to protect the communications is engaged in effective participation with the U.S. and its allies in mutual defense matters, the systems will be adjudged insecure and action may be instituted to bring about an improvement.

3. In each case in which corrective action is under study, steps will be taken, before such action is initiated, to assure that the physical and personnel security of the other government concerned are such as to prevent so far as practicable the leakage of classified information from those sources.

4. For communications among allied military commands in which there is U.S. participation and for which there has been no previous need for cryptographic systems but in which there will be future requirements for secure communications, action may be initiated by the U.S. to provide suitable means of making such communications secure.

5. Responsibility for initiating any actions which this policy may require is placed upon the Director, Armed Forces Security Agency, in his capacities as Chairman, Armed Forces Security Agency Council, and as Coordinator, United States Communications Intelligence Board.

In one draft I had added:
"In no case will any action intended to lead toward the improvement in the communication security of allied foreign government be taken if the action will jeopardize U.S. Comsec."
4177

Inclosure 1 with UC # 000321 dated 27 Aug 52.

TOP SECRET

~~TOP SECRET - SECURITY INFORMATION~~

BRIEF HISTORY OF THE PROBLEM
COMSEC VERSUS COMINT

1. The question as to which of two cryptologic aspects of tele-communications should be considered paramount to U.S. national security, in cases where U.S. communications intelligence (COMINT) interests and U.S. communication security (COMSEC) interests conflict, has come before U.S. authorities a number of times in recent years but the question has always been considered in connection with specific cases; it has never been studied attentively as a general or basic issue.

2. The question entered into the deliberations of the United States Communications Intelligence Board (USCIB) early in 1948, when the Department

[redacted]

ing on 2 September 1948 the NSC considered the problem but decided that it would take no action with regard to the subject brought before it by USCIB.

3. In a memorandum dated 30 June 1949 the Chairman of ISIB informed

[redacted]

Inclosure 2 with UC # 000321 dated 27 Aug 52.

In the course of the 1952 U.S./U.K. COMSEC Conference in Washington, the Director, AFSA, was advised by the head of the U.K. delegation that the British cabinet considered COMSEC paramount [redacted] and that the British delegation was acting under this policy. In its first comment on the LSIB memorandum, USCIB set forth certain reservations and presented an alternative solution which USCIB considered to be of "least detriment to [redacted]". However, the alternative solution was unacceptable to LSIB. After lengthy discussions, USCIB notified LSIB on 17 September 1949 that USCIB withdrew its objections to the British plan to issue TYPEX to the Western Union nations. However, USCIB's acceptance of the British plan was based upon the understanding that the TYPEX machines to be issued to Western Union nations would be specifically limited in their use, viz., (a) to encrypt "METRIC" communications only, and (b) that these would largely be military communications at Supreme Command and Governmental level in connection with Western Union Defense matters, the latter being a limitation which was explicitly stated in the very first paragraph of the LSIB memorandum of 30 June 1949.

4. Later, when the Western Union idea expanded into the North Atlantic Pact, the subject of secure communications for NATO entered into the picture. A U.K. proposal to issue the TYPEX MARK II to NATO countries for NATO communications was accepted by the U.S. but in a memorandum dated 19 October 1949 the Department of State made a reservation:

> "The Department of State member of USCIB feels that the British offer should be accepted provided that the use of these crypto-materials is specifically limited to those military communications of the signatory nations that concern North Atlantic Pact defense matters."

5. A short time after the use of TYPEX was approved for highest level NATO communications it was recognized that certain purely national communications at the same level, containing COSMIC information or references thereto, ought to be encrypted in systems of security higher than that afforded by those employed by certain NATO governments. For this reason permission was granted to the NATO governments to use the TYPEX for such purely national communications also, and an offer was made to instruct the governments concerned in the proper methods of compiling their own national key and key-lists. However, not much advantage has thus far been taken by those governments to receive such instruction and to avail themselves of the possibilities.

6. For intermediate or second-level NATO communications the U.S. authorities late in 1949 decided to recommend supplying NATO governments with the CCM, a decision later accepted by the U.K. authorities. However, the distribution of the CCM's and the circumstances under which they are to be used at this level are such that it is valid to assume that the communications to be encrypted will be practically all military, not diplomatic messages.

7. The preceding history establishes the fact that in agreeing to provide secure machines for Western Union and for NATO powers, there was always the reservation and understanding that they would be used for military Western Union "METRIC" or for NATO "COSMIC" communications, and not for purely national diplomatic communications of any of the powers involved.

8. The question of the use of U.S. or U.K. crypto-machines for non-military communications of NATO powers first came into the picture with the consideration of the [redacted] case. After rather lengthy preliminary discussions between USCIB and LSIB beginning in August 1948 and intermittently continued until April 1949, a formal U.S./U.K. conference on the subject was held in Washington in May 1951. The final report of the conference was considered by USCIB on 24 May 1951, at which time it was decided to forward the report to the National Security Council for approval because of the repercussions which the recommendations of the conference would have, if implemented, on U.S. [redacted] sources. The report did not explicitly raise, as a general or basic issue, the question as to which is more important to our national security, [redacted], in cases where these opposing interests are involved; it dealt specifically with the problem of [redacted] communication security. In forwarding the report to NSC this basic issue was not raised in the covering memorandum USCIB 14/137. In its decision the NSC did not raise nor answer the question, since the decision (USCIB 14/189) merely states that "the President ... has this date approved the conclusions and recommendations contained in the report of the USCIB-LSIB representatives ..."

9. The NSC action in the [redacted] case may warrant the conclusion that the NSC decision in that case can be taken as a policy-setting decision. However, the question is of such vital concern to U.S. national interests that it would be better to have the decision on record in the form of a clear-cut statement of policy for general guidance, rather than in the form of an implication derived from a single NSC action in a specific case.