

USCIB: 12./15

~~HANDLE VIA COMINT CHANNELS ONLY~~

24 May 1955

~~SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Cryptographic Assistance [redacted]

Reference: USCIB 12./10 of 26 October 1954.

1. Enclosed herewith is a copy of the recommendations of the Director, NSA with regard to the reference. The S-DMICC has concurred in the assumptions and proposed action set forth in paragraphs 6 and 7 of the enclosure. However, the USCSB has not yet agreed to the enclosed recommendations, the Army member having commented as follows:

"a. In recommending adherence to the policy adopted for the [redacted] NSA appears to favor a refusal of the [redacted] request, since only intra-[redacted] requirements (no inter-US [redacted] requirements) are involved. Such action would not take into account other important aspects of the problem as indicated below.

b. Our interests with respect to communications security of our SEATO allies correspond to those with respect to NATO (although SEATO, unlike NATO, is purely a political organization, it could change overnight into a military organization).

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

c. We should consider establishment of a Combined Working Group (US-Australia-UK) to study COMSEC problems of SEATO, with a view to protecting classified information which may affect seriously U.S. security if leaked through faulty communications of SEATO nations.

d. Immediate COMSEC assistance to the [redacted] [redacted] for intra as well as inter communications is considered in the best interests of U.S. The U.S. should adopt a policy of such assistance, even though shortage of equipment and priorities may make fulfillment of requirements difficult.

e. This problem should also be discussed by USCIB in view of their interests in certain aspects of any effort to improve SEATO COMSEC. There is also a requirement to notify the U.K. of any such arrangements that may be contemplated.

f. The policy with respect to [redacted] should be changed to permit immediate strengthening of their COMSEC, intra as well as inter, as the situation in [redacted] could change very suddenly."

USCIB: 12./15

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

USCIB: 12./15


~~SECRET~~

Subject: Cryptographic Assistance

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

2. The Chairman, USCSB would be grateful for the views of USCIB on the above prior to consideration of the matter in the USCSB. In this connection attention is invited to the fact that USCIB has not as yet informed USCSB of the purpose and activities of its Combined Working Group and Ad Hoc Committee for the Improvement of NATO National Communications Security. This occasion may be opportune for that purpose.

3. Owing to the heavy agenda of USCIBEC and the need for early consideration of the major policy aspects of the above quoted comment by the Army, this matter will be placed on the agenda for discussion at the next regular meeting of USCIB. In order to assist USCIB in arriving at a decision, comments by the State Department and NSA members of USCIB are requested for circulation to the rest of the members by Friday, 3 June 1955.


RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure
Copy of NSA Serial 2965-A
of 3 May 1955.

USCIB: 12./15

~~SECRET~~Serial: 2965-A
3 May 1955~~SECRET~~

MEMORANDUM FOR THE MEMBERS, USCSB

SUBJECT: Cryptographic Assistance to the [] Army

1. In October 1954, the Assistant Chief of Staff, G-2 Intelligence, U. S. Army, forwarded to the Director for appropriate action a message request from the Chief, JUSMAG, [] for cryptographic assistance to the [] Army. Copies of this request were circulated to the members of USCSB and USCIB under cover of COMSEC 2-18/1 (USCIB 12./10), dated 26 October 1954.

2. As you no doubt observed, the request was much too general to permit an evaluation of the nature or extent of the [] requirement. Consequently, on 5 November 1954 the Director requested that further details be furnished, specifically:

a. Were the cipher devices and publications to be used between United States and [] units, or by [] units only?

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

b. What were the expected echelons of use?

c. What specific cipher devices, JANAP's, and ACP's were considered appropriate, and which of those considered appropriate could be furnished by the U. S. Army?

3. In response to this request, a representative of Army Security Agency, Far East, visited Headquarters, JUSMAG, [], in December 1954 to obtain the necessary information. His report dated 17 February 1955, which was forwarded to this Agency by the Chief, Army Security Agency, letter, file GAS24 413.46, dated 17 March 1955, is summarized below for your information:

a. The [] have little knowledge of cryptographic principles, and any requirement which may be generated for the [] Army must of necessity include not only the provision of cryptosystems and operating instructions, but also communications security training.

b. At the present time, the requirement for enciphered communications exists only between [] military units, primarily Army units. There is a possibility, however, that a requirement may be developed for communications between the [] units and United States units in []

SECRET

~~SECRET~~

Serial: 2965-A
3 May 1955

c. Although the provision of security on [] Army circuits is desired only on those from Headquarters down to and including division size units, it appears that increased security is required also in the lower tactical echelons of the [] forces. Multilingual operations codes would be a probable solution.

d. It will be very difficult to adapt standard communications security equipment for the encipherment of the [] language. Attempts to convert the [] language to phonetic equivalents using the English alphabet have been unsuccessful, since only about 25% of [] military personnel are able to read English characters. Arabic numbers, however, are generally understood, and it is suggested that [] characters or words be converted to numerical equivalents prior to encipherment.

e. No teletype equipment is currently being used by [] military units, although it is planned that a certain amount of this equipment will be made available through the Mutual Defense Assistance Program (MDAP). It is not known what system will be devised for the use of this type of equipment with respect to the [] language.

4. In forwarding this report, the Chief, Army Security Agency, observed that the language problem and the lack of teletypewriter communications limit cryptographic assistance at the present time to simple pencil and paper systems. Based on this determination, he listed the following requirements:

a. A multilingual OPCODE for communication intra- [] and possibly inter [] S. use.

b. [] numerical one-time pad.

c. Authentication systems.

d. JANAP's, ACP's and other publications containing operating instructions and format required for the cryptosystem(s) released for use to the [] Army.

5. In addition to the above statement of requirements, Chief, Army Security Agency, inquired as to the extent of encouragement and/or assistance to be given in the development of teletypewriter equipment adaptable to the [] language.

6. The Director feels that in this matter he should be guided by the policy recently approved by USCSB in connection with a similar request for cryptographic assistance to the []

This policy established the principle that the United States would not undertake to provide cryptographic assistance for use in [] intra-governmental communications. The [] requirement, as stated in subparagraph 3b above, exists at this time only

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

~~SECRET~~

Serial: 2965-A
3 May 1955

for [] Army internal communications. It is assumed that USCSB will apply the same policy to [] as to [], and the Director has so informed the Chief, Army Security Agency.

7. Should a requirement develop, either as a result of [] participation in the Manila Pact or other circumstance, for inter [] U. S. secure communications, it is assumed that USCSB will consider the Director authorized at that time to provide low-echelon OPCODES, one-time pads, authentication systems and necessary publications, including ACP's. If additional requirements develop or assistance other than the above is requested, the matter will be referred to USCSB for consideration.

8. Confirmation and approval by USCSB of the assumptions and proposed action in this matter are requested.



JOHN B ACKERMAN
Major General, US Air Force
Acting Director