24

USCIB: 29.2/10

20 September 1954

~~SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Disclosure of Details of ROCKEX to the French.

1. The enclosure is forwarded for consideration by vote sheet at the request of the Director, National Security Agency. It is requested that vote sheet replies be returned to this office by 1200, 28 September 1954.

2. The enclosure has been distributed to members of USCSB for information.

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

Enclosure
Memo from Director, NSA
to Members of USCIB,
dtd 13 Sep 1954

USCIB: 29.2/10

13 SEP 1954

~~SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB

SUBJECT: Disclosure of Details of ROCKEX to the French

1. The use of national one-time systems for the encryption of NATO TOP SECRET, NATO SECRET, and all COSMIC messages is forbidden without specific Standing Group authorization. This has forced the U. K. Foreign Office to use a NATO approved cipher machine at installations where use of the U. K. cipher machine ROCKEX would have been more convenient and secure. The Foreign Office is therefore anxious that the U. K. obtain Standing Group approval for the use of ROCKEX for all classifications. To obtain such approval, full details of the equipment must be disclosed to the French. The Director, GCHQ, has approved such disclosure and similar approval by U. S. authorities has been requested by the British Cryptographic Liaison Officer in Washington.

2. ROCKEX is a one-time tape device for use with appropriate teletypewriter equipment. The one-time tapes used are composed of five-letter groups with appropriate line feed and carriage returns inserted at fixed intervals. Six-level tape is used. This tape meets the minimum tape standards promulgated by the Standing Group. Other details of the equipment and tape are as follows:

a. The ROCKEX mixer is designed so that cipher output consists of 26 letters. This is arranged by a feature which causes key letters to be transmitted directly whenever plain text plus key would yield a functions character as the cipher result. The plain-text character involved is added to successive letters of key until a literal cipher result is produced. In decipherment, the "by-passed" key letters are recognized since they decipher as BLKS. BLKS are not used in the plain-text input.

b. Tapes are divided into 49-group segments with each 50th group composing a segment indicator. Each tape contains approximately 26^3 letters.

c. The machine has radiation characteristics similar to SIGTOT.

d. Some machines are provided with tape-slitters to prevent reuse of key tapes.

e. Tape reels are equipped with special bosses which prevent the use of DECIPHER tapes for encipherment.

~~SECRET~~

3. Release of the equipment itself for use by NATO nations other than the U. K. is not contemplated at the present time since there is no surplus of ROCKEX machines. The basic cryptoprinciple used in ROCKEX is the same as that used in already approved NATO one-time tape systems.

4. I can perceive no objection to disclosure of full details of ROCKEX to the French for the purpose indicated and, in the absence of objection on the part of any other member, I will inform the British of USCIB concurrence.

RALPH J. CANINE
Lieutenant General, US Army
Director