~~SECRET~~

WDGSS-83

23 October 1945

SUBJECT: Declassification Patent Application Serial No. 443,320

TO: Chief, Security Division

(noted but not necessarily approved-MGJ)

1. The attached paper considers the problem of declassification of Patent Application Serial No. 443,320.

2. Recommendation is made that the patent application not be declassified.

3. Informal discussion with Commander Weeks, OP-20-K, who discussed the problem with Captain Smith, OP-20-Y, indicated concurrence with the recommendation.

4. It should be observed that, contrary to the statement of Mr. Friedman's letter, only in part are the principles of the patent application utilized in the Converter M-294. There are rotors involved in producing a keying sequence in the Converter M-294 but the manner of combining the key and plain-text signals in this device is not the same as in the Converter M-228, described in subject application.

2 Incls
1. Ltr 27 Sep 45
2. Study

/s/ L. M. Myers
Lt. Col., Signal Corps
Chief, Communications
Security Branch

~~SECRET~~

Cir 1

~~CONFIDENTIAL~~

~~Suspense~~
~~20 Sept 45~~
19

27 September 1945

SUBJECT: Release of Patent Application Serial No. 443,320

TO: Commanding General
Army Security Agency

1. The subject patent application covers a cryptographic means and device for automatic encipherment and decipherment of teletypewriter signals and was filed in the U. S. Patent Office on 16 May 1942 in the name of the undersigned and Frank B. Rowlett, as co-inventors.

2. The principles involved in the subject application have been utilized in Converter M-228 and Converter M-294.

3. It is requested that the subject application be officially declassified in order that it may be allowed to go to issue, whereupon the right and title will revert to the undersigned and Frank B. Rowlett, subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America.

4. This action is desired because of the commercial applications of the invention, interest in which is believed to exist on the part of the U. S. communication companies.

5. Declassification of the patent application does not necessarily involve the declassification of the specific embodiments thereof represented in the apparatuses mentioned in paragraph 2.

WILLIAM F. FRIEDMAN

Inclosure 1

CONFIDENTIAL

~~SECRET~~

PROBLEM PRESENTED:

1. Should declassification of Patent Application Serial No. 443, 820 be authorized.

FACTS BEARING ON THE CASE:

2. The device as described in the patent application is similar to the Converter M-228 but incorporates two features not present in the Converter M-228. In addition, the application does not state specifically the type of control to be employed in the mechanism of the subject patent for advancing the rotating switches (rotors).

a. Provision is made for varying the number of input points to be energized, and the number may be accomplished by the operator at any specified time.

b. The five output leads may be permuted in any of 120 ways, also at the will of the operator.

c. The application states that stepping or advancement of the rotating switches can be done in a number of ways, either periodic or aperiodic, and that the manner of doing this are well known in the art.

3. Although the specific application of the principles stated in the patent application is not embodied in the Converter M-228, it appears that the claims of the inventors include the specific case of the Converter M-228, with the exception of the stepping control.

4. Many persons in the Army and Navy are familiar with the principles described in the subject application, as employed in the Converter M-228, and could duplicate similar mechanisms because of such knowledge. There is now in Congress, however, a bill which, if passed, would place a definite

~~SECRET~~

Incl 2

control on release of any information of a cryptographic or cryptanalytic nature gained while employed by the U. S. Government or in the Army or Navy.

5. The Converter M-228 has been made available to the British Government so that at the present time the principles are not the exclusive knowledge of the U. S. Government.

6. Means of enciphering teletype signals have been well known for several years. Supplying a keying sequence for encipherment may be accomplished by either of two methods:

a. A previously prepared key for use in the device, such as perforated tape or tapes.

b. A mechanical means of producing key which may be connected to a teletype and used as required.

The first method has been known for several years and is available in a commercially manufactured cryptographic device (Telekrypton). The second method is not known to have been utilized until the subject patent application described one way of utilizing a mechanism attached to a teletype. As indicated in the patent application, the mechanism employs rotating switches (rotors) to produce a long non-repeating key. The Germans are known to have used a mechanical means of producing a keying sequence for enciphering teletype signals but based upon a different principle. The principle used by the Germans is analogous to the action of the key wheels in the Converter M-209.

7. The cryptographic systems used by the U. S. Government represent the highest level in the world with respect to security and practicability of operation. With regard to the security of systems attention is directed

to Memorandum for Colonel Corderman, dated 13 March 1945, subject: Security of our high-grade cryptographic systems. The conclusion stated therein is "They (Germans and Japanese) cannot read and are not reading our high-grade cipher traffic."

8. Declassification of the method, thereby making it available to anyone who examines the patent, or should commercial models become available, making it possible to examine these, may result in raising the cryptographic level of other nations. On the other hand secure devices (the commercial Enigma) was available before the war to anyone wishing to make the purchase.

9. On 19 September 1945, the Army Security Agency recommended to Chief, WIB, that the request of a foreign government, desirous of obtaining assistance from the War Department in establishing a system of secure codes and ciphers, be unfavorably considered.

10. Should declassification of subject patent application be authorized a precedent will be established regarding declassification of high-grade cryptographic systems.

DISCUSSION:

11. The two features of the patent application differing from the Converter M-228 appear to afford greater security against unauthorized reading of messages. If the Army and Navy adopt these features for incorporation in the Converter M-228 and the patent application is declassified all elements of the patent would be present in the Converter M-228, except the manner of stepping the rotors.

12. Means of imparting a periodic or aperiodic motion to the rotors are not specified but the application states that methods considered as well known in the art may be used. It would be possible to utilize the

methods of the Converter M-134-C to produce an aperiodic motion in the rotors, or the method presently employed in the Converter M-228, or variations of these methods. Such methods, if well known, have not been used to the best advantages by other nations, if at all.

13. If the bill now before Congress is passed and becomes law, revelation of the nature of the Converter M-229 or principles similar in nature to the Converter M-229 may be prohibited.

14. Although there are available now to any interested parties certain cryptographic devices which offer a high degree of security, new principles and finished designs undoubtedly will tend to raise the cryptographic level of other nations and this could impede materially progress in fulfilling the mission of Intelligence Division of the Army Security Agency.

CONCLUSIONS:

15. Efforts are being made to protect the "trade secrets" and "know how" of U. S. cryptographic systems. Declassification of subject patent application would be opposed to this policy. There is little evidence available to show that other nations are so advanced in cryptographic matters. Consequently, release of knowledge gained by efforts of U. S. personnel would be of benefit to other nations.

16. Other cryptographic systems employed by the U. S. Government may have commercial applications and declassification of subject application would establish a precedent difficult to overcome if similar requests are made on patents of other cryptographic systems.

RECOMMENDATIONS:

17. That no action be taken to declassify Patent Application Serial No. 445, 820.

Ch, Gen Processing Br.....(93)
Ch, Facilities Br.....(94)
Ch, I & D Br.....(95)

( ) Approval & Return
( ) As Requested
( ) Concurrence or Comment
(✓) Information & Forwarding
( ) Information & Return
( ) Information & File
( ) Recommendation
( ) Signature if Approved
( ) Your Action (by_____)
( ) For recommended reply

You may be interested in
pages 68 - 80.

J

Gen Clarke has seen
JTB

CSGAS 96 (Rev. 14) 15 Apr 49 8-411

REF ID:A104786

These are extra copies + copies of things never sent.

J