

STAFF STUDY ON CONVERTER M-325 (SHORT TITLE: SIGFOY)

PROBLEM PRESENTED

1. That plans should be promulgated for the distribution and use of the Converter M-325

SRH - 007

FACTS BEHIND THE CASE

2. A "Stylar-Operated Keyboard for a Roll Paper Recorder" was conceived by the Principal Cryptanalyst, ...

3. The Signal Corps Patent Board determined that the invention is of value to the Army and that the specifications to the Patent Office should be prepared.

STAFF STUDY ON CONVERTER M-325

(SHORT TITLE: SIGFOY)

4. In November 1947 approval was granted for the Principal Cryptanalyst, to patent the keyboard, since the Patent Section had not filed the application. The Signal Corps Patent Section initiated action in December 1948 to file the patent application. The action, however, was not carried through to completion. The patent application for Converter M-325, Case No. 545026, was filed 11 August 1948.

5. Manufacture of Converter M-325 was completed in 1948. The machine is used for ... for establishing ... keyboard similar to that conceived by Principal Cryptanalyst ...

DECLASSIFIED per Part 3, E. O. 12356
by Director, NSA/Chief, CSS

TRD Date: 11 August '87

STAFF STUDY ON CONVERTER M-325 (SHORT TITLE: SIGFOY)

PROBLEM PRESENTED

1. What plans should be promulgated for the distribution and use of the Converter M-325?

FACTS BEARING ON THE CASE

2. A "Stylus-Operated Keyboard for a Small Portable Cryptograph" was conceived by the Principal Cryptanalyst, United States Army on 1 August 1935.

3. The Signal Corps Patents Board determined on 26 May 1936 that this item is of value to the Government and recommended that the inventor submit specifications to the Patent Section, Office of the Chief Signal Officer.

4. In November 1937 approval was granted to permit the inventor, personally, to patent the keyboard, since the Patent Section had delayed filing the application. The Signal Corps Patent Section initiated action 6 December 1941 to file the patent application. The action, however, was not carried through to completion. The patent application for Converter M-325, Case No. 549086, was filed 11 August 1944.

5. Nomenclature "Converter M-325" was assigned 5 June 1943 to a machine designed for enciphering messages in the combat or field code and for authenticating stations engaging in radio communications. It employs a keyboard similar to that conceived by Principal Cryptanalyst 1 August 1935.

W-49-44-3

Do Not Destroy. Return to the
P.S. Library when no longer needed.
Copy No. 1

DECLASSIFIED
Authority NND 947022

~~SECRET~~

RECORD COPY
DO NOT DESTROY OR MUTILATE

6. Military characteristics for Converter M-325 were approved 20 July 1943 by Signal Corps Technical Committee. (See Tab A).

7. The Converter M-325 was assigned the short title SIGFOY on 1 March 1943.

8. The following Army requirements for the M-325 were estimated 19 April 1943:

Armies	18	per Headquarters
Corps	12	" "
Divisions	6	" "
Air Forces	16	" "
Bomber Commands	8	" "
Fighter Commands	8	" "
Air Support Commands	8	" "
Wings	2	" "
Military Attaches	2	" "
Posts, Camps, Stations	2	" "
Theaters of Operations	10	" "
Base Commands	8	" "
Service Commands	5	" "
Antisubmarine Commands	5	" "
Antisubmarine Wings	3	" "
Ports of Embarkation	3	" "
Fixed Radio Stations	2500	Total for all Stations

Requirements	9224
20% Maintenance Factor	1845
10% Distribution Factor	<u>922</u>
Total Requirements	11991

On 23 June 1943 a contract was let for twelve thousand (12,000) Converters M-325. A contract for 24,000 sets of rotors for M-325 was placed 6 November 1943. This quantity was based on an estimated need of 2 sets of rotors for each converter.

9. An order was placed 17 May 1944 for one thousand (1000) M-325 and two thousand (2000) sets of rotors for the Navy Department.

10. Letter of 8 May 1944, from the Secretary of War to the Secretary of State approves the issue of one thousand (1000) M-325's and two thousand (2000) sets of rotors to the State Department. This letter further states that the first priority will be accorded the State Department in the distribution of this equipment.

11. War Department Approval of "Keying Instructions for Converter M-325" (Short title SIGLAN-1) was received 30 May 1944.

12. A Purchase Request for spare parts, amounting to \$45,824.25, was made 6 July 1944.

13. Converter M-325 has been demonstrated to the Army Air Forces and the Army Ground Forces. Both services expressed a need for and an interest in the use of the Converter M-325. Correspondence, requesting statements of interest from these services, was sent 21 August 1944.

14. To date, 5725 Converters M-325 have been delivered. One thousand (1000) more are expected in the very near future. The balance of the machines are scheduled for delivery by the end of November 1944. As of this date, 1787 sets of rotors (short title SIGNAL) have been received. The balance should be delivered by the end of November 1944.

15. As of this date 625 Converters M-325 and 624 sets of rotors have been issued to the State Department. The balance of 376 rotors have been wired and are ready for issue. Request for the second thousand rotors has not been received from the State Department.

16. Action was taken 5 September 1944 by "C" Branch to implement the cancellation of 1,500 Converters M-325, 3,000 sets of rotors, and the Purchase Request for spare parts in the amount of \$45,884.25.

DECLASSIFIED

Authority

NND 947022

This decision was based on the premise that the Army's requirements for the M-325 would be diminished by the possibility of imminent cessation of hostilities in the European area. The parts for 1500 converters will be available for use as replacement parts, thus making the Purchase Request for spare parts unnecessary.

17. The Converter M-325 was designed for dual operation as a "cryptograph" and as an authentograph". Various methods of utilizing the M-325 for the latter purpose have been discussed, however, none of them have met the complete requirements. An attempt was made to have the "AUT-CIP" switch removed from the converter but production was too far advanced to accomplish this.

DISCUSSION

18. It was originally intended that the initial trial operation of the Converter M-325 would take place among the military attaches in North Central and South Americas. This was to be followed by the introduction of the M-325 in the Caribbean Defense Command. The converters were issued to the attaches along with a letter explaining the initial operation. (See Tab B). The distribution of associated material has been delayed by the necessity for making further changes in "Keying Instructions for Converter M-325", short title SIGLAW-1. While this document has been in the process of revision Converters M-325 have been issued to the Antilles and Panama Canal Departments of the Caribbean Defense Commands.

The operation of the M-325 in the Caribbean Defense Command is to be comparable to that undertaken by the military attaches. It is contemplated, however, to extend the trial operation to a period of six full weeks and to arrange for the reversing rotor to be rewired during the course of the operation. A letter, similar to Tab B, will be sent to all holders of M-325 in the Caribbean Defense Command. That headquarters has approved a request that an officer from the Signal Security Agency be present during the six weeks trial operation. It is contemplated that Captain Douglas will visit in the Caribbean area to observe the operation and to render any assistance necessary. Final arrangements cannot be made until SIGLAW-1 is completed. Distribution is due to be initiated within a month. "Maintenance Instructions for Converter M-325" (Short title SIGDARA) is ready for issue. Associated systems for use by the military attaches and by the Caribbean Defense Command are being prepared and should be completed before SIGLAW-1 is completed. It will take approximately one month to complete distribution of M-325 and associated documents to all holders in the Caribbean Defense Commands. Therefore, initial operation in that area can be expected to begin early in November. It is probable that the military attaches can begin using the M-325 shortly before that time.

19. Steps are being taken to remove Persian Gulf Command from distribution lists for systems in Cryptonet 19, and establish a new cryptonet, number 41, for that command. It will provide a system for use with the Converter M-325. Distribution of the net, and Converters

DECLASSIFIED

Authority NND 947022

M-325 will be held in abeyance until SIGLAW-1 is available for issue. No formal report will be submitted on the initial weeks of operation of the M-325 in the Persian Gulf Command.

20. It is contemplated that the M-325 will replace strip cipher where the latter is used for normal or stand-by cryptographic systems. This will cancel the requirements for double transposition systems with regard to the general cryptographic plan (cryptonets), since strip cipher will be available as a replacement for emergency use. The M-325 will first replace those strip systems carrying the heaviest traffic load or information of greatest significance. It is believed that no further attempt should be made to introduce the M-325 in other parts of the world until the results of the operation by the attaches in the Western Hemisphere and by the Caribbean Defense Command have been studied. Based on the results of these trial operations, any necessary changes in the systems and instructional documents may be made.

21. It is considered advisable to defer the replacement of the strip systems in Cryptonet 16 until that time, with the highest priority given to replacement of systems used by military attaches in the Far East.

22. The following figures are available on traffic cryptographed in theater strip systems:

<u>Headquarters</u>	<u>System</u>	<u>No. of Groups per day</u>
Alaskan Dept. USAFIFE	1822	6,000
	2022	4,000 - (20,000 when new base is opened - prior to use of ABA)
Antilles Department SOPAC	2702	3,150
	2122	1,000

<u>Headquarters</u>	<u>System</u>	<u>No. of Groups per day</u>
ETO	2221, 2222	578.2
Persian Gulf Comd.	1923	550
NATO	2421, 2422	300
Panama Canal Dept.	2722	275
USAFINZ	1921, 7922	100

23. Based on the above data, it would appear logical to plan distribution of the M-325 according to the following sequence:

- Alaskan Department (Cryptonet 18)
- U. S. Army Forces in Far East (Cryptonet 20)
- U. S. Army Forces in China Burma India (Cryptonet 23)
- Army Air Forces (Cryptonet 17)
- Pacific Ocean Area (Cryptonet 21)
- Posts, Camps and Stations (Cryptonet 15)
- European Theater of Operations (Cryptonet 22)
- North African Theater of Operations (Cryptonet 24)
- U. S. Army Forces in Middle East (Cryptonet 19)

24. Final plans for training should be made when the results of the trial operation are known; since detailed aspects of the method of operation may be changed as a result of this trial.

25. Two training cryptonets for use by the Crowder and Monmouth Theaters of Operations are being prepared. These nets will contain M-325 systems. In addition the present Cryptonet 10 will be revised for use as a universal net to be held at both Crowder and Monmouth. The revised net will also contain an M-325 system. One hundred (100) copies each of an M-325 system will be furnished the schools at Crowder and Monmouth for classroom use. Due to the necessity for ironing out certain details in the structure of the nets, it is difficult to establish a date when

these training cryptonets will be ready for use. October 15, 1944, however, has been suggested as a probable date.

CONCLUSIONS

26. That action should be taken to standardize the Converter M-325 when statements of concurrence in the proposed use of the converter are received from the Army Air Forces and the Army Ground Forces.

27. That final arrangement for the initial operation of M-325 by the military attaches in the Western Hemisphere cannot be made until SIGLAK-1 is ready for issue. The setting up of a new cryptonet (number 41), including M-325 systems, in the Persian Gulf Command is also dependent upon the completion of SIGLAK-1.

28. That no further action should be taken in distributing M-325 until the results of the operations mentioned in the previous paragraph have been studied. Since the results will probably be known and analyzed by the latter part of December, plans can be made at that time for introducing M-325 systems into the other cryptonets.

29. That the priority of future issues of M-325 be determined by the amount of traffic loads carried by respective strip systems and the importance of the information being transmitted thereby.

30. That a plan for training be prepared by Director of Training and action be taken to include the M-325 in service schools when the results of the trial operation are known and when standardization of the converter has been effected.

DECLASSIFIED

Authority NND 947022

RECOMMENDATIONS

31. It is recommended that approval be granted to place the following plan into effect:

a. Step One

When concurrences in the proposed use of the M-325 have been received from the Army Air Forces and the Army Ground Forces, action will be taken to effect the standardization of the Converter M-325.

b. Step Two

When SIGLAW-1 is ready for issue the following action will be effected:

(1) Trial Operation of the Converter M-325 by the military attaches and the Caribbean Defense Command.

(2) Distribution of a new cryptonet to Persian Gulf Command, containing an M-325 system.

(3) Use of training cryptonets at Camp Crowder and Fort Monmouth, providing for operation of M-325.

(4) Inclusion of the Converter M-325 in the training program of the service schools.

c. Step Three

When the results of the trial operation by the military attaches and the Caribbean Defense Command are known, and any necessary changes in the operation of the converter have been established, arrangements will be made to include M-325 systems in the following cryptonets in the order indicated below:

DECLASSIFIED

Authority NND 947022

- (1) Cryptonet 18 (Alaskan Department)
- (2) Cryptonet 20 (U. S. Army Forces in Far East)
- (3) Cryptonet 23 (U. S. Army Forces in China Burma India)
- (4) Cryptonet 17 (Army Air Forces)
- (5) Cryptonet 21 (Pacific Ocean Areas)
- (6) Cryptonet 15 (Posts, Camps, Stations)
- (7) Cryptonet 22 (European Theater of Operations)
- (8) Cryptonet 24 (North African Theater of Operations)
- (9) Cryptonet 19 (U. S. Army Forces in Middle East)

d. Step Four

When the action outlined in Steps One, Two, and Three has been completed, requirements for double transposition systems can be removed from the general cryptographic plan, although it will remain an authorized type of system for special purposes.

COORDINATION

32. Necessary coordination with the Personnel and Training Division and the Development Branch of the Security Division is being effected.