

WDGSS-72

14 December 1945

SUBJECT: Army Ground Forces Equipment Review

TO: Chairman, ASATC

1. This memorandum summarizes the comments of the Ciphony Sub-Committee of the ASATC on the Army Ground Forces Equipment Review Board Report. The memorandum is divided into four parts as follows:

- I. General Comments
- II. Comments on Specific Paragraphs of the Subject Report
- III. Comments on the Statements Made by the Theaters and Other Agencies on the Subject Report
- IV. Summary of the Present Status of the Ciphony Program

I. GENERAL COMMENTS

2. The stand taken by the Army Ground Forces Equipment Review Board with regard to ciphony equipment may be summarized as follows:

- a. An integrated secure telephone system should be the primary means of tactical communication.
- b. Adequate secure and light weight ciphony equipment is the predominant need in achieving such a communications system.
- c. Development of improved ciphony equipment should be given the highest priority.

3. The Sub-Committee concurs in the importance of ciphony equipment and in the necessity of giving its development the highest priority. The speed, convenience and the advantages of direct personal contact obtained with voice communication are fully recognized by the sub-committee. However, certain facts must be considered before a final decision is reached to use voice communication as the primary means of tactical communication.

4. The complex nature of speech results in serious technological difficulties which must be overcome before both secure and light weight ciphony equipment can be pro-

~~SECRET~~

~~SECRET~~

WDGSS-72 (14 December 1945)

vided. At the present stage, secure equipment can be provided but such equipment is large and complex. Present light weight equipment is insecure and inadequate in other respects. It must be recognized that no solution is now in sight which will entirely overcome the problems involved and that it will probably be some years before equipment which is both small and secure enough to be used on the very widespread basis contemplated by the Ground Forces can be developed. Furthermore, severe compromises in the remainder of the communications system may be required to accommodate such improved ciphony equipment.

5. Another factor to consider in the widespread use of ciphony equipment is the lack of a permanent written record. In the case of SIGSALY, a high echelon secure ciphony device, it was found necessary after a period of use to install recorders for this purpose.

6. In view of the above, it is recommended that the development of ciphony equipment be continued with the highest possible priority with the aim of ultimately achieving the results desired by the Ground Forces while, at the same time, continuing a considerable program to develop improved, more convenient and faster literal cipher systems.

7. One important decision which must be made in connection with the application of ciphony to an integrated communications system concerns the plan used in applying ciphony to the system. Two general plans are possible:

a. Ciphony equipments located at the users with no intermediate ciphony devices.

b. Security for each link in the system provided by separate ciphony equipments. This would mean that when a call passes through several switchboards, ciphony equipments located at the switchboards (and at the users) would secure each link in the system independently.

8. While (a) above is the more desirable alternative from a security viewpoint, since the users can be certain that adequate security is being maintained over the entire system, the difficulties in providing and operating the system make it thoroughly impractical. Cryptographically communicable ciphony devices would be required at every telephone. This will only be possible when a very small but highly secure device is available. Furthermore, every user would have to be in possession of the key settings

~~SECRET~~ 2

~~SECRET~~

WDGSS-72 (14 December 1945)

required to communicate with every other user with whom he must communicate. This is obviously impractical in a highly integrated system from both security and operational viewpoints. A further objection to this plan is the inflexibility which would result. It is therefore recommended that plan (b) or a compromise between plans (a) and (b) be adopted.

9. The Board report has very little to say with regard to Cifax equipment. It seems likely that a need, perhaps not clearly recognized at the present time, exists for a cifax device for transmitting classified maps, sketches, photographs, etc. The Cryptographic Plan (SIGIRA) includes requirements for two types of cifax devices: (a) A portable device for use in forward echelons and (b) A fixed plant device for use between higher headquarters.

II. COMMENTS ON SPECIFIC PARAGRAPHS OF THE BOARD REPORT

10. Par. 89b - Preproduction models of Speech Equipment AN/GSQ-3 are now in the hands of this Agency and tests on them will be completed by 15 March 1946. This equipment partially fulfills the requirement for equipment for Army Corps and Division nets but does not meet the military characteristics included as Inclosure 3R of the Board Report. The nomenclature, Speech Equipment AN/GSQ-5, has been assigned equipment to meet the military characteristics. Pilot models will be available in not less than two years. Speech Equipment AN/GSQ-4 to meet the military characteristics (Inclosure 2R) for equipment for Regimental, Battalion and Company nets is now under development, but pilot models will not be available for several years.

11. Par. 106a - Concur.

12. Par. 106b - Concur. However, in general no difference between equipment for use on radio and wire should be contemplated.

13. Annex R, Par. 1b - Concur in so far as the need for speech security is expressed.

14. Annex R, Par. 2c - See paragraphs 3,4,5 and 6 above.

15. Annex R, Par. 3b - Concur. However, in general no difference between equipment for use on radio and wire should be contemplated.

SECRET

~~SECRET~~

WDCSS-72 (14 December 1945)

16. Annex R, Par. 3c - Development work on these equipments has already been started. See Paragraph 10 above.

III. COMMENTS ON STATEMENTS OF THEATERS AND OTHERS

17. LTO Comments, Par. 89a - Concur with one exception--no inherent security is available in any radio equipment, including AN/TRC-6.

18. LTO Comments, Par. 89b - Concur. However, due to the technical problems involved in the development of such equipment, it is unlikely that light weight equipment of medium and high security can be provided for a considerable period of time. In the immediate future, equipments will be either large in size or relatively insecure.

19. LTO Comments, Par. 89g - Concur in the need for enciphered facsimile. If RC-5 is used to transmit the plain text of written messages, some means of enciphering the transmitted signal should be provided. It is not felt, however, that the cipher device should be built into the facsimile equipment, but rather that the facsimile and cipher equipment should be of functionally integrated design. See paragraph 9 above.

20. ETO Comments, Par. 3 - Concur in statement as a general policy. Exceptions may be required in specific cases, however.

21. USAFP Comments on Specific Paragraphs 1 and 2 - Concur in the importance of speech security.

22. USAFP Comments on Specific Paragraphs, Par. 5k - Military Characteristics, Inclosure 2A, ACP Equipment Review Board Report, covers equipment which will fulfill these requirements. It is not recommended that combined radio-telephone and voice security equipment be provided.

23. SCEL Comments, Par. 106b - Concur. See paragraphs 3, 4, 5 and 6 above.

24. APPACF 41/1c - This statement is interpreted to mean that a secure ciphony device should be provided for use with such a system. Concur that security would be required for such a system.

IV. PRESENT STATUS OF DEVELOPMENTS

A. Historical Introduction

~~SECRET~~

~~SECRET~~

WDGSS-72 (14 December 1945)

25. Since the outbreak of the war, active interest in ciphony equipment on the part of the using services has become increasingly apparent. The first recognized need for speech security equipment which resulted in the development of a highly secure device was for equipment to secure radio-telephone circuits between Washington, D.C. and the various theaters of operation. The equipment developed to fill this need was Telephone Terminal RC-220-T1 or SIGSALY.

26. The SIGSALY is a very large, intricate device, consisting of approximately 50 seven foot individual bays and requiring fixed plant installation in buildings capable of being air-conditioned. Air-conditioning apparatus is included as a part of each terminal.

27. The equipment has served its purpose very adequately. The cryptographic principles utilized are sound and the development and use of the equipment has proven to be a significant stepping stone in the advancement of the art of speech security.

28. By the spring of 1942, it was apparent that there were definite requirements for speech security equipment, not only in the high-level echelons with which SIGSALY was associated, but also in Army Corps, Division and lower. At this time the Army Communications Board investigated the requirements (Case No. 77, "Security of Voice Communication over Wire and Radio Circuits"), proposed military characteristics for three types of speech security equipment, and recommended their development. These were:

Type I - Equipment for use forward of the Division, offering two (2) hours of security. Equipment should not weigh more than 50 pounds, should not occupy more than $1\frac{1}{2}$ cubic feet and should not require more than 150 watts of primary power.

Type II - Equipment serving headquarters of Divisions, Corps, Armies and Task Forces offering 72 hours of security. Equipment should be capable of being installed and operated in a standard $2\frac{1}{2}$ -ton Cargo truck with a trailer for primary power supply.

Type III - Equipment serving headquarters of Theaters, Defense Commands, Major Commands and the War Department offering 12 months' security and be operable as terminal equipment in fixed plant installations.

29. The recommendations of the Army Communications Board were approved by the Assistant Chief of Staff, G-4, and concurred in by the Assistant Chief of Staff, G-2.

~~SECRET~~

~~SECRET~~

WDGSS-72 (14 December 1945)

It was directed by G-4 that the recommendations of the board be carried out as expeditiously as possible.

30. The requirement for Type III equipment had already been filled by SIGSALY. It was then necessary to develop the Types I and II devices. Nomenclature was assigned as Speech Equipment, AN/GSQ-1, for the Type I equipment and Speech Equipment, AN/GSQ-2, for the Type II equipment. (Later, the AAF requested that two Type II equipments be furnished; one installed in a shelter, and the other packed for air shipment. The former was designated as Speech Equipment, AN/GSQ-3).

B. Present Status

31. Speech Equipment, AN/GSQ-1, which was developed in an attempt to meet the requirements for Type I equipment, is a device operating on the time-delay-scrambling (TDS) principle. The Army Ground Forces became interested in it after a demonstration before the Infantry Board at Ft. Benning in March, 1945. It was decided by the Army Ground Forces that it would be acceptable as an interim device and would be issued on a T/O and E basis to Army Ground Forces units. At the time hostilities ceased, plans were being made with the manufacturer for large-scale production. At present, specifications are prepared, test data are available and the equipments may be manufactured if the need should arise.

32. The principle faults of the equipment are:

- (1) It does not offer sufficient security.
- (2) It can be used only on a push-to-talk circuit, due to the inherent time delay of the system.
- (3) It is too large and requires too much power to be used as a man-carried device.

33. Speech Equipment, AN/GSQ-3, which has been under development in an attempt to meet the requirements of Type II equipment, is a miniaturization of the SIGSALY equipment. Contracts were placed for six (6) service test or pre-production models, and two (2) of these have been delivered. By 15 March 1946 all six (6) will have been delivered and engineering and service tests will have been completed.

34. Before the cessation of hostilities, the Army Ground Forces indicated a substantial requirement for

~~SECRET~~

~~SECRET~~

WDGSS-72 (14 December 1945)

Speech Equipment, AN/GSQ-3. Again, arrangements were being made with the manufacturer for large scale production, the equipment being accepted by the AGF as interim device. After V-J Day, the procurement program was cancelled and nothing further has been done toward scheduling procurement to provide the equipment to tactical troops, although the equipment has been standardized.

35. The AN/GSQ-3 fell short of the military characteristics as set forth for Type II equipment in the following respects:

- (1) The equipment is much larger and heavier than called for by the M/C's. Installation is made in a large 4-wheel trailer with the power unit carried by the towing tractor (a $\frac{1}{2}$ -ton Cargo truck).
- (2) Special microphones are needed (these are furnished as part of the equipment).

36. The equipment exceeds the M/C's with regard to security requirements, in that the security offered is comparable to that of the SIGSALY. The size of this equipment could not be appreciably reduced by lowering the security.

C. Current Plans

37. Both Speech Equipment, AN/GSQ-1 and Speech Equipment, AN/GSQ-3 have fallen into the category of interim devices for the Army Ground Forces because of the recent requirements which became evident early in 1945. These are set forth in military characteristics prepared by the Army Ground Forces and forwarded to the Army Security Agency in March 1945. The two equipments required by Army Ground Forces have been assigned the nomenclature of Speech Equipment, AN/GSQ-4 and Speech Equipment, AN/GSQ-5 (Inclosures 2R and 3R, Army Ground Forces Equipment Review Board Report).

38. At the present time, research work is being conducted with high priority in order that the two equipments may be expeditiously developed. Several proposals for the AN/GSQ-5 show promise and these are being diligently studied. Work on the AN/GSQ-4 has consisted of preliminary research and, as yet, no method for providing the

~~SECRET~~

~~SECRET~~

WDGSS-72 (14 December 1945)

necessary security with the size and, as yet, no method for providing the necessary security with the size and weight limitations has been revealed. The work continues on this basis.

39. Every effort is being made to keep abreast with the trend toward miniaturization and functional integration of Army communications equipment. From the development of the SIGSALY to the projected plans for Speech Equipment, AN/GSQ-5, great strides have been accomplished. It is expected that, although no immediate solution is evident for the smaller equipments, more secure and somewhat smaller devices may be developed in the next few years.

DANIEL F. HOTH
Captain, Signal Corps
Chairman, Ciphony Sub-
Committee

~~SECRET~~