LIST OF QUESTIONS RELATIVE TO ARMY AIR FORCES MILITARY CHARACTERISTICS FOR COMMUNICATIONS SECURITY EQUIPMENT

General Questions or Items for Discussion

1. Does Army Air Forces plan to leave to Army Security Agency the decision as to whether a device built in accordance with the M/C's is to be an integrated or non-integrated equipment?

2. Many suggestions will probably be made with regard to training periods on all the AAF equipment. Under the army enlistment system it is necessary that consideration be given to the portion of an enlistment period given to training for a job and certainly the AAF should express themselves on this point. This training time should be minimum consistent with other requirements. However, where the use of a device is intended to be such as to require extremely short and simple training periods, specific reference to this requirement should be given, with indication of the priority of this requirement as compared to requirements for security, weight, size, speed, etc. For instance, with the M-209, where operators are constantly being shot up, to be replaced by mere novices, with no training to speak of, the requirement for simple maintenance and operation training takes precedence over security, as does weight and size. In this respect, the Chief, Technical Staff (TSAF-R1) proposed to AAF and Research and Development Division in April 1946, that all future M/C's be written much like a newspaper story, with first things first. Abbreviations of the M/C's by cutting from the end then leaves the essential requirements expressed in the first paragraph, and a delineation of these in order of decreasing importance as the end of the presentation is approached.

Specific Questions or Items for Discussion

3. Master Encrypted Transmission System.

a. Present planning considers this system for use only between ar

LIST OF QUESTIONS RELATIVE TO
ARMY AIR FORCES MILITARY CHARACTERISTICS
FOR COMMUNICATIONS SECURITY EQUIPMENT

General Questions or Items for Discussion

1. Does AAF intend to permit AAA to decide whether (a) the devices fashioned after the M/Cs will consist of consolidated crypto and communications equipment or (b) they will be crypto-attachments for existing communications equipment?

2. Many suggestions will probably be made with regard to training periods on all the AAF equipment. Under the army enlistment system it is necessary that consideration be given to the portion of an enlistment period given to training for a job and certainly the AAF should express themselves on this point. This training time should be minimum consistent with other requirements. However, where the use of a device is intended to be such as to require extremely short and simple training periods, specific reference to this requirement should be given, with indication of the priority of this requirement as compared to requirements for security, weight, size, speed, etc. For instance, with the M-209, where operators are constantly being shot up, to be replaced by mere novices, with no training to speak of, the requirement for simple maintenance and operation training takes precedence over security, as does weight and size. In this respect, the Chief, Technical Staff (TDCAS-81) proposed to AAF and Research and Development Division in April 1946, that all future M/C's be written much like a newspaper story, with first things first. Abbreviations of the M/C's by cutting from the end then leaves the essential requirements expressed in the first paragraph, and a delineation of these in order of decreasing importance as the end of the presentation is approached.

Specific Questions or Items for Discussion

3. Master Encrypted Transmission System.

a. Present planning considers this system for use only between War

Department and theater headquarters. Unless AAF is organized as a separate service, a device under BTR II, XI or IX might well fulfill the contemplated requirements of the AAF.

b. Suggest that in paragraph 1 the term "infinite security" might be replaced by appropriate delineation of "high security" much like the reference in BTR I, Ground Point-to-Point Section of SIGIRA. Security Division is reluctant to consider security in terms of infinity.

c. In paragraph 2f (T/C's) suggest "Operate with standard applicable types of signal communications equipment."

4. High-Medium Echelon Literal System.

a. Indication here is for a "black box" that can be used with normal applicable standard Teletypewriter equipment. The "black box" should in no way "prevent" delivery of standard page or tape copy from this equipment, nor hinder the operation of the standard equipment at the speed of modern printing telegraphy. Since planning for the future includes 100-150 speed equipments in the teletype field, some "cover" phraseology to guarantee this rapid operation should be included.

b. Reference paragraph 2j (T/C's). Further explanation of "normal teletypewriter power supply" is desirable.

c. Reference paragraph 2f, (T/C's). It is considered that the direct encryption of numerals, while itself feasible, would cause considerable difficulties in the operation of such a device. The fact that transmission errors will occur in some degree would necessitate the repetition of each numeral in any message. When transmission is by radio, this is almost certain to result in message delays and loss of channel time. Errors that may occur in single characters of numerals that are spelled out, however, will not normally cause requests for re-

peats. A repeated numeral actually requires a second repetition, if the first repetition differs from the original transmission, in order to determine which is correct. However, tabulations cannot be handled by spelled out numbers as well as by directly encrypted numerals.

5. Low Echelon Literal System.

a. Reference paragraph 2a (W/C's). Suggest substitution of "Be capable of emergency operation from standard battery supply."

b. Security of this device should be expressed as adequate in terms of the echelon of use. Policy on this matter should be promulgated and the W/C's revised by AAF in accordance with the policy if possible.

c. Reference paragraph 2g (W/C's). See paragraph 4c above.

d. Reference paragraph 2j (W/C's). What is meant by standard military power sources?

6. Airborne Literal System.

a. Paragraph 4a above applies generally here.

b. Reference paragraph 2j (W/C's) paragraph 4c above applies.

c. For reasons unknown, specific power supply references are not made.

d. Security should be considered on terms of the approved policy, as adequate for the echelon considered.

7. Special Mission System.

a. Suggest rephrasing of "infinite" security.

b. Reference paragraph 2b (W/C's) recommend substation of "capable of multiple conference operation."

c. It is understood that paragraph 2h (W/C's) means that AAF does not want to be limited as to message lengths for each indicator used . . . . they do

not want to have to string out a series of short messages to get a predetermined message length for sending with a given indicator, nor do they wish to have to break or otherwise curtail lengths of messages sent under one indicator. But the wording does not clearly convey this thought.

d. How does "mobile airborne-operation" differ from "airborne operation"?

e. Paragraph 4c above applies.

f. Further consideration might be given to utilization of a common device for W/C's 5 and 4, Special Mission System and Airborne Literal System. If this is practicable the advantages are obvious.

8. Aircraft Movement System.

a. Reference paragraph 2d (W/C's) "Tape" should be modified. Is printed or punched tape or both intended?

b. Reference paragraph 2e (W/C's) paragraph 4c above applies.

c. Reference paragraph 3d (W/C's) what is meant by "Normal Code Room Personnel? Paragraph 2 above applies.

d. Further amplification of paragraph 1 (W/C's) required.

9. Weather Collecting System.

a. Reference paragraph 1 (W/C's) is not weather traffic sent in all classifications during war time?

b. Reference paragraph 2j (W/C's) What are the present and anticipated airborne power supplies? Voltages, etc.?

c. Specific reference should be made to a requirement for manual and automatic on-line, and off-line operation.

10. Medium-High Echelon Ciphony System.

a. Reference paragraph 1 (W/C's) How about Top Secret?

b. Paragraph 2c (W/C's) might be more clearly stated to indicate that

c. Reference 3c ("/C's) Suggest maximum weights, sizes, etc. be given. That is, or more appropriately, what will be the limitations as to weight and size placed on items to be transported by "standard cargo aircraft"?

11. Airborne Ciphony Equipment.

a. Reference paragraph 2b ("/C's) Since the cryptographic equipment will supply a signal for modulation only to the radio transmitter and since the transmitted signal will therefore be a characteristic of the radio transmitter and not of the ciphony converter it is rather difficult to see how the converter may supply a signal that will not be unduly affected by atmospherics and interference.

b. Reference paragraph 2i ("/C's) Vague. Does this mean standard airborne power supply? If so, what are standard airborne power supplies? What trend will they take in the future?

c. Reference paragraph 2k ("/C's) The airforce equipment would be held by ground force units with which the Air Force unit wished to communicate. This equipment supplies a signal for modulation by HF line-of-sight command radio sets, whereas normal ground units cannot use HF line-of-sight transmissions except for short distances or to aircraft. Therefore the AAF equipment would work with identical equipment issued to AGF units that need it.

d. Reference paragraph 2p ("/C's) "Minimum "lag" probably would do better than "no lag" if technical correctness is desired.

12. High-Medium Echelon Cifax Equipment.

a. Reference paragraph 2a and 2f ("/C's) These might be stated thusly:

Not adversely affect the traffic handling capacity, operating range, or intelligibility normally afforded by any transmission system with which it is used.

b. Reference paragraph 2j (M/C's) Information is not sufficiently definite. Normal voice circuits may be split as to bandwidths, that is, having bandwidths of 1600 CPS and circuits of this type will not permit facsimile transmission. This characteristic might properly state definitely the permissible frequency allocation.

c. Reference paragraph 2c and 2d (M/C's) Here, again, the "black box" idea is advanced. The security equipment should not, when used with facsimile equipment that can meet 2c and 2d (M/C's), in any way prevent the facsimile equipment from doing this. Perhaps a rewording is in order.

13. Airborne and Low Echelon Ciphax System.

a. Reference paragraph 2a and 2f (M/C's) see paragraph 12a above.

b. Is this to be as "integrated" or "black box" type of equipment?

c. Reference 3b (M/C's) There is that "mobile airborne operation again!!

d. Security should be expressed in terms of the "adequate" policy paper, or at least an understanding should be reached.

14. Would it be advisable to try to standardize the order of presentation of the information much in the manner used in preparing the two redrafts attached as TAB A and B? Can consideration be given at this time to writing the M/C's with "first" things first? Obviously, in some M/C's weight and size are more important than degree of security or speed of operation and vice versa. Can some expression of this relation be included in the M/C's?

2 Incls
1. M/C's for Medium-High Echelon Ciphony System (TAB A)
2. M/C's for Airborne Ciphony System (TAB B)

MILITARY CHARACTERISTICS FOR MEDIUM-HIGH ECHELON CIPHONY SYSTEM

CONVERTER _____

1. GENERAL REQUIREMENTS

Air Forces has a requirement for voice secrecy equipment for command and conference purposes among high and medium echelons. This equipmsnt will be designed to afford security from enemy analysis to voice wire and radio communications of classifications including SECRET and TOP SECRET.

2. OPERATIONAL CHARACTERISTICS

This equipment shall:

a. Not adversely affect the traffic handling capacity, operating range, or intelligibility normally afforded by any transmission system with which it is used.

b. Be so constructed that knowledge of the general crypto-systems and/or possession of the equipment will not compromise the security of the communications.

c. Be so constructed so that the specific key may be readily changeable by the operating personnel.

d. Emit a clear, strident warning to both subscriber and attendant when transmission in the clear is occurring.

e. Be provided with a simple emergency destruction means.

f. Operate successfully with appropriate types of standard military radio sets intended for voice transmission and with wire telephone equipment having a transmission band width of at least 3000 cycles per second without modification of either.

2. OPERATIONAL CHARACTERISTICS (Cont'd)

g. Be operable from a standard telephone handset if consistent with other characteristics.

h. Provide for multi-station net operation.

i. Provide for multi-subscriber operation off one terminal.

j. Be operable from a 115/230 volt 50/60 cycle power source and be provided with a standard power plant capable of continuous operation.

k. Be operable with corresponding Army Ground Forces equipment.

3. PHYSICAL CHARACTERISTICS

a. The converter shall be light, sturdy, compact and of the simplest possible design consistent with other requirements.

b. The converter shall be housed in a submersion-proof carrying-case or cases which are of a sufficiently rugged and weather-proof construction to withstand normal usage in the field.

c. The converter and power source shall be transportable in any standard cargo aircraft.

d. All components shall be so constructed as to be capable of operation and storage under all climatic conditions to be encountered in the field.

e. The converter shall be separable into components each not to exceed a two-man load.

f. It shall be capable of being installed by two men.

g. It shall not require close control of ambient temperature by operating personnel.

h. It shall be capable of being installed and operated in any shelter suitable to the installation of comparable communications equipment.

4. TRAINING REQUIREMENTS

The training for operating and maintenance personnel for this equipment shall be the minimum consistent with other requirements.

MILITARY CHARACTERISTICS FOR AIRBORNE CIPHONY SYSTEM

CONVERTER _____

1. GENERAL REQUIREMENTS

Air Forces has a requirement for voice secrecy equipment for use in low echelons point-to-point, air-to-air, and air-to-ground communications providing security to include the minimum classification of CONFIDENTIAL and which is an integral part of aircraft command communications equipment.

2. OPERATIONAL CHARACTERISTICS

This equipment shall:

a. Not adversely affect the traffic handling capacity, operating range, or intelligibility normally afforded by any transmission system with which it is used.

b. Be so constructed that knowledge of the general crypto-systems and/or possession of the equipment will not compromise the security of the communications.

c. Be so constructed so that the specific key may be readily changeable by the operating personnel.

d. Be an integral part of aircraft command radio equipment.

e. Be operable from a standard microphone.

f. Provide for multi-station operation.

g. Be operable from standard power available in military aircraft.

h. Not require constant control of synchronization.

i. Be operable with Air Forces equipment when held by Ground Forces.

j. Be usable for point-to-point low echelon voice traffic.

k. Be capable of handling highly stereotyped air-to-air and air-to-ground voice weather messages.

2. OPERATIONAL CHARACTERISTICS (Cont'd)

l. Require that there shall be no lag between the time of reception and the time of transmission.

m. Be provided with a simple emergency destruction means.

3. PHYSICAL CHARACTERISTICS

a. The equipment shall be capable of being installed in any military aircraft.

b. The equipment shall be capable of being operated and stored under all climatic conditions to be encountered in the field.

c. The weight of cryptographic element should not exceed 15 pounds.

4. TRAINING REQUIREMENTS

The training for operating and maintenance personnel for this equipment shall be the minimum consistent with other requirements.