~~TOP SECRET~~

COPY

DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
Washington 25, D. C.

AFSA-11/meb

~~TOP SECRET~~

JUL 18 1951

MEMORANDUM FOR AFSA-12

Subject: Comment on USCIB 13/195, "Measures for the Increased Security of COMINT"

1. AFSA-11 recommends that we take the position of supporting the principles of this proposal while reserving judgement on details. This is a logical position to take, because it would be useless to belabor the details (some of which need second thoughts) until we have some assurance that the general principles on which they are based have general U. S. acceptance.

2. In my opinion, these principles are forced on us whether we like them or not. The basic purpose of the new proposal is to increase the security of really top-level, really sensitive COMINT, and to increase the usefulness of lower-level, less sensitive COMINT. It is proposed to do this by separating the two, and handling them differently, so that the high-level, sensitive COMINT will not be imperilled by association with low-level COMINT which requires wide dissemination, and the low-level COMINT will not be sewed up to the point of uselessness by association with high-level COMINT which requires stringent safeguards. Unless you separate them, you will not accomplish this purpose.

3. The salient feature of the new proposal, then, is the method of division of COMINT into separate categories. The proposed categorization can be called a departure from or not a departure from the basic principles of the present Appendix B depending on how far down you go in your definition of "basic". The original 1946 Appendix B provided for dividing COMINT into categories based broadly on difficulty of production. The proposed version does the same thing, so that there is really no departure from the old principle in that respect. Where the difference lies is in the direction of slicing the categories. The original division was a horizontal one--cryptanalysis was difficult, so it formed the top category, with greatly limited dissemination--traffic analysis was less difficult, so it formed the lower category, with less restricted dissemination. (I ignore for the moment the fact that, in practice, no difference was made in degrees of dissemination.) Thus, with any specific body of foreign traffic, you could cryptanalyze it and disseminate the product narrowly as top-category COMINT, or traffic-analyze it and put out the product more widely as low-level COMINT.

4. This basis of categorizing began to come loose at the seams almost as soon as it was devised. The nature of the problem was such,

COPY

TOP SECRET

~~TOP SECRET~~

MEMORANDUM FOR AFSA-12 JUL 18 1951

Subject: Comment on USCIB 15/195, "Measures for the Increased Security of COMINT"

or began to become such, that the neat distinction between difficult, sensitive cryptanalysis and easy, insensitive traffic analysis simply did not hold. This was recognized in 1948 in amendments to Appendix B by which exceptional shifts of category could be made for specific cases of "easy" cryptanalysis and "difficult" traffic analysis. This makeshift seemed to patch up the old Appendix B almost adequately for a while, but the plain language problem and various problems brought out by the Korean War, and which have been partially solved on a piece-meal basis, have shown that a more fundamental change is needed.

5. The present proposal provides for a vertical category division by technical difficulty and sensitivity of the foreign communications themselves, rather than by what is done with them. This statement, though an oversimplification, is essentially true. Of course, the proposed top category will continue to contain largely the products of cryptanalysis, and very few of traffic analysis, and the bottom category will be heavily traffic analysis--but this will be because of the nature of things, and not because of artificialities created by category definitions, as at present. (Under the proposal, categorization, in practice, will be specific--for each new COMINT job as it comes up someone will have to determine what category it belongs to. At present, the category is prescribed by blanket rules which, as often as not, fail to satisfy the needs in individual cases.)

6. The details of <u>how much</u> we are going to take the wraps off the low-level stuff, and what the code-words will be, and how handled, and whether there shall be one level of clearance or two or four, require some study, and I do not propose to go into that now. It seems to me that USCIB must agree (1) that the four proposed categories are necessary, (2) that the higher ones must come under rules predicated on <u>high security</u>, and (3) that the lower ones must come under rules predicated on <u>usefulness</u>. This much agreed on, we should present these basic points to ISIB, to get their reaction. Only then need we start haggling over the details of implementation. The proposed revised Appendix B submitted with the paper is merely one way of doing it--there are many others.

/s/ E. S. L. Goodwin
E. S. L. GOODWIN
Captain, U. S. Navy
AFSA-11

CC: AFSA-OOB

TOP SECRET