~~SECRET~~

~~SECRET~~

A8-6(2) Security of AFSA communication circuits

AFSA-04 AFSA-00A 5 May 50

1. The attached memo from AFSA-00B, dated 14 April 1950, is forwarded for your comments and recommendation.

cc: AFSA-13

/s/ S.P. COLLINS
S.P. COLLINS
Colonel Signal Corps
Deputy Director, AFSA

To: AFSA-00A From: AFSA-04 Date: 23 MAY 50 Comment No. 2
Mr. Corry/426

1. Surveillance of communications intelligence activities has been largely limited in the past to occasional spot-checks because of limitations on personnel available for such tasks and because of the tremendous scope involved in a thorough analysis. A rough estimate indicates that AFSA communications represent at least 75-80 percent of the total encrypted message volume of the Armed Forces. Included among activities conducted recently along this line are:

a. Approximately a year ago, one traffic analyst was assigned the task of determining types and amount of information available through external examination of Army Security Agency traffic. Coverage was limited to ASA traffic appearing on ACAN circuits which were under surveillance for ordinary security monitoring purposes. No formal report was rendered but evidence was sufficient to indicate that the following conclusions could be substantiated:

(1) That the peculiar characteristics of intercept traffic make it easily identifiable and that any attempt at concealment would have to be of such drastic nature as to make practicability questionable.

(2) That it is probable that the extensive use of radio communications for forwarding of intercept is unjustified, and that proper segregation and use of courier aircraft would result in reducing radio traffic volume to such an extent that consideration feasibly might be given to application of transmission security measures to reduce recognizability.

(3) That the Army Security Agency field intercept organization (i.e., "Order of Battle Information") could be reconstructed with a minimum of effort.

(4) That some "special" operating practices which tend to further segregate intercept traffic might be eliminated without impeding traffic handling.

~~SECRET~~ COPY

~~SECRET~~

~~SECRET~~
File No. A-8-6(2) Subject: Security of AFSA communication circuits
To: AFSA-OOA From: AFSA-04 Date: 23 MAY 50 Comment No. 2
Mr. Corry/426

(5) That circuit discipline and operator efficiency, although approximating the overall Army level, could stand considerable improvement.

(6) That establishment of a procedure whereby the security monitoring activity might insure that corrective action is taken in cases of major transmission security violations, would be beneficial.

(7) That, under certain circumstances, it is possible for an enemy to determine specific intercept targets by careful padding of his traffic volume and close analysis of volume originated by certain intercept stations.

(8) That, by observation of volume originating in certain areas, it is possible for general areas of emphasis for intercept purposes to be determined.

b. Within the past year and a half, Op-20ZK conducted a survey of Communication Supplementary Activity Traffic similar to that carried on by Army Security Agency. The conclusions were adequate; not only was "Order of Battle Information" obtained but the classified call signs and delivery groups in use on the supplementary net were recovered in full.

c. Stations originating intercept traffic have been subject to the same violation, compromise, and traffic volume reporting procedures as all other Armed Forces activities, thus providing one means of continuing surveillance. It was in connection with the carrying out of this procedure that the recent decisions concerning the inadequacies of CSP 1515/SIGGUM were determined.

d. A program to avoid association of direct connection between certain "critical area" Special Security Officers and Arlington Hall Station has been in effect for some time. This program involves careful control of external addressing of communications and, in some cases, use of disguised cryptographic system indicators.

e. Spot-checks of message headings of decrypted tapes have been made at irregular intervals in the past for indicator depths and for careless practices in indicator selection.

f. Re-evaluation of crypto-security provided by ASAM 2-1 has been in process for the past several weeks. An attempt is being made to devise a one-time key procedure acceptable for intercept station use.

~~SECRET~~ COPY

~~SECRET~~

~~SECRET~~
File No. A-8-6(2) Subject: Security of AFSA communication circuits
TO: AFSA-00A From: AFSA-04 Date: 23 MAY 50 Comment No. 2
Mr. Corry/426

2. It is believed that a more complete and more thorough security analysis of AFSA communications is desirable, to obtain factual data to substantiate conclusions presented in paragraph 2a bove, and to provide a planned check on cryptographic operating practices. This will require some assistance from AFSA-02.

3. It is recommended that the attached Disposition Form, requesting assistance from AFSA-02, be approved and forwarded.

1 Incl
D/F from AFSA-04 to
AFSA-02 subj as above

/s/ H.O. HANSEN
H.O. HANSEN
Captain, U.S. Navy
Chief, Office of Security

~~SECRET~~

COPY