

~~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

- (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-202K 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 GSP 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~~

JUPY

~~SECRET~~~~SECRET~~

File No. A-8-6(2)

TO: AFSA-OOA

From: AFSA-04

Subject: Security of AFSA communication circuits

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 above, 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