5 opense to 15 May

~~SECRET~~ SECRET

AFSA-00X/ef

26 April 1951

MEMORANDUM FOR AFSA-00B

SUBJECT: Crypto-Security of AFSA Communications

1. I agree with AFSA-02 that the Crypto-Security of AFSA Communications should be under continuous or periodic scrutiny, but I agree with AFSA-00B that this should be done by AFSA-04, as a matter of assigned responsibility, rather than by the creation of another panel or committee. I also agree with AFSA-02 that using MINERVA (ASAM 2-1) for purposes other than forwarding of raw intercept traffic presents a potential danger.

2. I cannot concur in the statement that vital intelligence will be gleaned through traffic analysis of COMINT circuits. The Russians know full well we are intercepting their communications just as we know that they are intercepting ours. Every radio station is a potential intercept station and its potentialities are in direct proportion to its size. Traffic analysis of COMINT circuits can only give unimportant negative information: certain radio stations are not forwarding intercept traffic via radio. It does not indicate that the station could not be used for intercept purposes in the future or might not be forwarding intercept material by means other than radio. Traffic analysis will give confirmation of facts which the Russians already well know, but this is neither vital nor particularly detrimental to either AFSA or the United States.

3. The pressing need of the moment appears to be restricting the COMINT use of MINERVA (ASAM 2-1) to the forwarding of raw intercept material and providing other systems for daily coverage reports, orders and instructions from AFSA, translations, etc. MINERVA, of course, could be used for re-encryption of the latter. Also, one-time encryption should be introduced in the forwarding of raw intercept material if not already in use.

L. F. SAFFORD
Captain, USN
AFSA-00X

Copy to:
AFSA-00A
AFSA-00T
AFSA-04
AFSA-02
AFSA-13

~~SECRET~~ SECRET