

- Suspense to  
25 April  
15 May

17 April 1951

MEMORANDUM FOR AFSA-OOB

SUBJECT: Crypto-Security of AFSA Communications

1. I am deeply concerned over the security of our COMINT communications from a cryptanalytic viewpoint. A cursory examination of this problem indicates that crypto-systems currently in use between AFSA and field organizations (i.e., theater processing centers and intercept stations) and from units in the field to main processing centers for the passing of raw intercept and COMINT may be subject to successful attack by enemy or foreign COMINT organizations. As an example MINERVA (ASAM 2-1) is used to forward raw intercept and daily coverage reports from field units to AFSA and from field units to theater headquarters. It is an accepted fact that this system can be successfully exploited cryptanalytically under certain conditions which may frequently occur. Likewise, equally vulnerable aspects of our communications may be exploitable through traffic analysis and vital intelligence gleaned therefrom.

2. The present complexity of the COMINT problem as a whole, emphasizes the need for maintaining a close security check on our own communications in order to minimize, if not entirely eliminate, the possibility of any knowledge of U.S. COMINT activities being made available to enemy or foreign COMINT organizations. The outbreak of hostilities in Korea, and particularly the entry of Communist China into the conflict made it necessary to readjust our COMINT effort. An expanded and accelerated program was instituted, as a direct result of which not only was the volume of raw intercept substantially increased, but providing for the rapid forwarding of additional volumes of traffic became an operational necessity. A concomitant growth was evident at once in the communications volume from AFSA to the field in order to direct this expanded intercept effort. As an example in June 1950 AFSA received by electrical means an average of 494,826 groups daily of raw intercept. By March 1951 this average had increased to 823,443 groups daily. A corresponding increase in volume has also taken place during the same period in outgoing groupage from AFSA. I think it also pertinent to point out that this already complex problem is steadily increasing in complexity and size. Long-range mobilization planning for AFSA has as its nucleus a greatly expanded intercept effort which will of course increase the amount of raw traffic available to AFSA and in turn increase the volume of communications among AFSA and field units and other processing centers. With this growth the need for maintaining a close watch on the crypto-security of our communications becomes even more necessary.

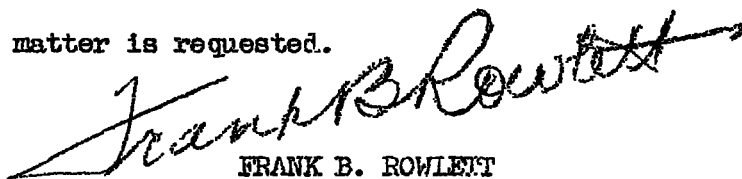
3. To the best of my knowledge it has been a long time, perhaps too long a time, since this matter has been looked into and discussions held among representatives of appropriate divisions of AFSA. It seems to me to be entirely worthwhile to review the entire problem; to ascertain the weaknesses, if any, in our present crypto-systems and their use and

SUBJECT: Crypto-Security of AFSA Communications

to formulate new procedures and techniques for coping with this task wherever and whenever the need appears. I believe that our vulnerability both from a traffic analytic and cryptanalytic viewpoint should be thoroughly explored. Indeed, the time is now ripe, for AFSA has been organized and operating for over a year.

4. Accordingly, I propose that a panel be established composed of representatives of AFSA-02, AFSA-04, and any other cognizant groups, to make a study of this entire problem and upon its completion to submit their findings and recommendations to DIRAFSA. I further propose that this panel be permanent and that it meet at stated intervals to review the vulnerability of AFSA communications to foreign COMINT effort and report its findings and recommendations.

5. Your guidance in this matter is requested.



FRANK B. ROWLETT  
Technical Director  
Office of Operations

cc: AFSA-00T  
AFSA-00X  
AFSA-04  
AFSA-13