29 August 1951

MEMORANDUM FOR AFSA-03 THRU AFSA-04 RCS

SUBJECT: Low echelon cipher machine

1. a. Currently, AFSA is developing two machines designed for low echelon use and not requiring electrical power:

(1) AFSAM-36 (The "MCM")

(2) DEM-17 (The pneumatic-powered model)

b. AFSAM-36 is a keyboard-operated "double Hagelin" device, with twice as many keying elements as the M-209. From the standpoint of practicability in operation (ease and rapidity of setting up the machine to the correct daily key and message setting), the MCM leaves much to be desired. I doubt very much whether our operators would be able to use the machine satisfactorily. Unless special procedures are introduced and rigidly followed, transmissions in depth or near-depth could be expected, weakening the system materially, or at the very least compromising the intelligence in the messages concerned. In short, in my opinion the development along the lines of a "double Hagelin" device represents our going up a blind alley. However, this development is so far along now that any substantial changes in design would delay its completion beyond a date acceptable to the Navy and especially the Marine Corps, the organization specifically desirous of having an all-mechanical crypto-machine for amphibious operations.

c. The DEM-17 is quite a long way from completion but it represents such a novel and promising approach to the problem that, in my opinion, the development should be expedited by all possible means.

2. The modified M-209, with irregular stepping of key-wheels and interlocking motion, which was recently submitted to us by Mr. Hagelin, represents a marked improvement in regard to security of M-209 traffic. Although it remains true that two identically-keyed messages can still be read by our usual procedures, recovery of pin and lug settings for the day remains a problem of considerable difficulty, if not beyond the realm of practicability with our present analytic machinery. Hence, although there would undoubtedly be occasional cases of solution, these would involve only two isolated messages in each instance and not the whole day's traffic whenever such an instance occurs, as is now the case.

3. Since the DEM-17 development represents an approach which offers promise but the outcome of which will be unknown for several years, and since it would be inadvisable to change the design of the present MCM to incorporate the modified Hagelin action described in Par. 2, I suggest that serious consideration be given to the question as to whether

SUBJECT: Low echelon cipher machine 29 August 1951

AFSA should embark upon a third approach to the problem, viz., to develop an all-mechanical machine embodying the modified M-209 (Hagelin) action in a small keyboard-operated machine. Such a development would provide insurance against the contingency (a) that the MCM will not stand up under the test of practical war-time usage and (b) that the DEM-17 development may also prove impractical. It appears that at least the Navy (Marine Corps) needs something better than the present M-209. Although neither the Army nor the Air Force has thus far submitted MC's for such a piece of equipment as the MCM, I believe that there is a need (which is currently being met by the present M-209) and that, as regards the Army, the need may become very urgent in the near future.

4. Although the patent situation is not clear with regard to U.S. ownership of a license to the Hagelin improvement under discussion, I do not think there would be any difficulty in reaching a satisfactory understanding with Mr. Hagelin, in case we should wish to use the principles underlying the improvement.

5. AFSA still has the experimental model of the modified M-209 sent by Mr. Hagelin last December and I promised recently to return it to him very soon. However, in view of this memorandum I will keep the model a few days longer, pending a determination as to whether it would be useful to retain it for purposes of discussing my suggestion.

6. Your comments are requested on the suggestion made in Par. 3; and in view of Par. 5, they should be forwarded as promptly as possible, so that I may know soon whether to ask Mr. Hagelin for an extension of the loan of the model.

William F. Friedman

WILLIAM F. FRIEDMAN
AFSA-OOT

Info. Copy to:
AFSA-OO )
AFSA-OOA ) in turn
AFSA-OOB )
AFSA-OOC )