~~CONFIDENTIAL~~

~~CONFIDENTIAL~~ 11 September 1951

MEMORANDUM FOR AFSA-03

SUBJECT: Low Echelon Cipher Machine

Reference: OOT's Memo to 03 thru 04, dtd 29 Aug 51

1. AFSA-04 agrees that the AFSAM 36 does not appear to be the ideal equipment for providing security for the communications of low echelons and that the development of the DEM 17 should be expedited by all possible means.

2. A comprehensive security evaluation of the modified M-209 has not been possible, since the model submitted by Mr. Hagelin possesses a number of engineering deficiencies which make it difficult to operate the machine in a dependable fashion. It would appear, however, from studies which have been made, that there may be security weaknesses in the sample model of the modified M-209 which might require modification of the cryptoprinciples. The lack of dependability of the model on hand does not permit a proper comparison of the operational facility of the modified M-209 with the AFSAM 36.

3. It would appear necessary, before making any decisions about possible research and development on Hagelin's modification, to obtain an operationally dependable model on which can be carried out a complete security evaluation.

4. Should the security evaluation prove that the modification does represent sufficient improvement, then AFSA-04 agrees that the development of an all-mechanical machine embodying the modified M-209 (Hagelin) action would provide some insurance against failure of both the AFSAM 36 and the DEM 17 projects to provide a satisfactory solution to the low echelon problem. It is therefore recommended that an effort be made to get from Mr. Hagelin, as soon as possible, a satisfactory model of his new design in order to permit a decision regarding the desirability of establishing a research and development project.

G. V. Johnson, Lt Col Sig C
for

R. C. SEARS
Colonel, U. S. Air Force
Acting Chief, Office of
Communication Security

CC:
OOT

~~CONFIDENTIAL~~