REF ID: A53627

JUINT AMERICAN MILITARY ADVISORY GROUP, EUROPE 20 GROSVEROR SQUARE LONDON, W. 1.

COEX

PC 311.5

9 Feb 1951

SUBJECT: Hagelin Machine Converter (Cipher), M-209-8 Armed Forces Security Agency TO: EO 3.3(h)(2) The Pentagon PL 86-36/50 USC 3605 Washington 25. D. C.

- 1. In consideration of the NATO code and cipher problem. the European NATO Tri-Regional Cipher Committee has provisionally set up the following categories of ciphers:
- s. Top Level Ciphers. To provide for the needs of high military and diplomatic authorities. This part of the problem is supposedly now solved by the provision of the British Typex Mark II Machine.
- b. Second Level Ciphers (strategic). To provide for the needs of units down to and including Air Force Groups, Army Divisions and major naval vessels.
- c. Third Level Ciphers (tactical). To provide for the needs of smaller headquarters and units.
- 2. On 30 January 1950 the Western European Region (NATO) Cipher Committee met in Paris to consider s for MATO adoption and joint use as a second-level cipher. This machine proved to be nothing more than a U. S. built. Army Signal Corps, Machine Converter, M-209-B.
- 3. The representative admitted that the M-209-B had virtually no security, but stated that if the machine were equipped with the modification described in enclosure 1 encrypted traffic would be "absolutely secure."
- 4. The representative explained that the proposed modification to the M-209-B was protected by patents and that it would therefore have to be manufactured by firms or by foreign firms under contract. He also stated that since the model being exhibited was only a prototype it would probably take about one year before all MATO units could be equipped with the modified M-209-B.

## SECRET

REF ID: A53627

EO 3.3(h)(2) RL 86-36/50 USC 3605

## SECRET

COEA	Ĺ	5.	Re	presentatives	were	requested	to	be	prepared	to	state
	at	the	next	meeting:			1	1			

- a. Whether their nations were prepared to accept, on a joint Army-Navy-Air Force basis, the M-209-B with the fication as a second-level cipher machine.
- b. Whether their nations were prepared to accept, on a joint Army-Navy-Air Force basis, the M-209-B in its unmodified form as a third-level cipher machine.
- c. Their nations' short and long term numerical requirements for the machine (if accepted) bearing in mind that priority should be given to international traffic.
- b. If, as is the opinion of personnel of this headquarters who have operating crypto experience, the U.S. position in regard to the \_\_\_\_\_\_ proposal will probably be one of non-acceptance, is any U.S. counterproposal available? This counterproposal might take the form of a definite U.S. commitment to release a comparatively secure system, such as a strip cipher with the strip eliminator table, or it might take the form of a firm Standing Group statement to the effect that the matter was under active consideration and that a solution was expected at some definite date in the near future. The opinion of this headquarters is that the \_\_\_\_\_\_ proposal is a retrograde step and should be overruled. This, however, may be difficult, since the M-209-B with the \_\_\_\_\_ modification is the only low-level cipher device now available to MATO, and the European nations may be inclined to adopt it for lack of something better.
- 7. U. S. information and guidance pertaining to the contents of paragraphs 5 and 6 above is required by the U. S. representative on the Cipher Committee prior to the next meeting on 27 February 1951.

A. FRANKLIN KIBLER Major General, USA Director

CC: JCEC CNO(DNC) G-2 (ASA) Dir. Communications (USAF)

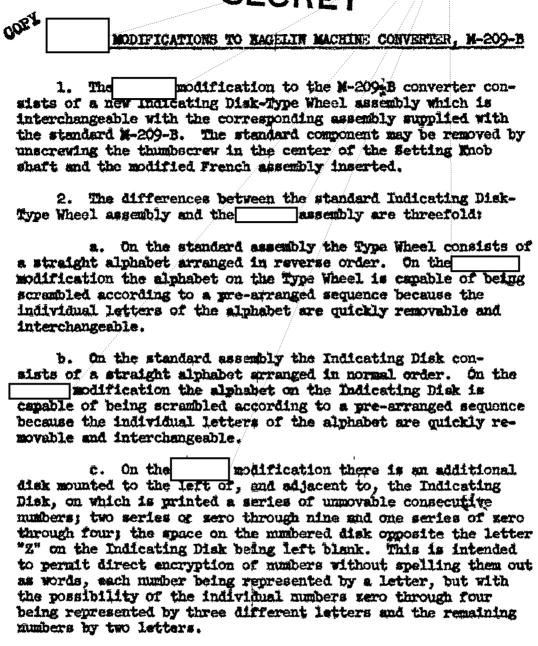
Enc. 1: Modification to M-209-B

SECRET

REF ID: A53627

EO 3.3(h)(2) PL 86-36/50 USC 3605

## SECRET



3. One feature which may be cryptographically undesirable is the fact that the letters "1" on both the Indicating Disk and the Type Wheel are always fixed in the same position relative to each other in order to form a common base for the scrambled Type Wheel and Indicating Disk alphabets employed.

Inclosure 1

SECRET