



~~SECRET~~

D R A F T

To: Assistant Chief of Staff, G-2, War Department General Staff,  
Washington 25, D. C., Attention: Lieutenant Colonel Goodrich

Mr. David A. Salmon, Special Consultant to the  
Assistant Secretary of State

1. Attention is invited to the attached communication from ~~the~~  
<sup>U.S. Army</sup> State Department requesting the issue of four (4) ~~M-134-A~~  
<sup>Converter Type M-134-A</sup> cipher machines,
2. Subsequent to the receipt of this letter, <sup>similar</sup> additional equipment  
<sup>the Embassies in</sup> was informally requested for installation at Stockholm and Lisbon.
3. Through informal contacts with the Navy, it has been ascertained  
<sup>U.S. Navy</sup> that the State Department requested HCM cipher machines for issue to  
their installations in Madrid, Stockholm, Lisbon, Istanbul, Ankara, Algiers,  
and Cairo. <sup>the</sup> Navy Department agreed to the installation of HCM cipher  
machines in Ankara, Cairo, Istanbul, and Algiers, but declined to issue  
the subject equipment for installation in Stockholm, Lisbon, and Madrid  
for security reasons.
4. The State Department, at present, has <sup>Navy</sup> HCM cipher machines in  
most of its South American installations. At the present time, the State  
Department has eight (8) <sup>Converter</sup> M-134-A cipher machines, of which four (4) are  
located in the United States Embassy in London and four (4) in the State  
Department in Washington. ~~The code room in which this equipment is located~~  
~~in London is operated by United States Army personnel.~~

5. ~~It is felt that it is necessary, to aid the State Department in~~  
~~to the best interest of the Government that the cryptographic security of the State~~  
~~maintaining cryptographic security of the highest order with respect to~~  
~~Department be of the highest order. For a number of years the Signal Security Agency~~  
~~its cryptographic communications, since the Army and Navy have competent~~  
~~under authorized directives, has been rendering technical advice and~~  
~~personnel and equipment capable of accomplishing this mission, it seems~~  
~~operational assistance in the production of cryptographic material~~  
~~wise that they should aid the State Department as much as possible so~~  
~~for the State Department, and in its proper maintenance and use, and as~~  
~~Very recently a review of the Department's cryptographic~~  
~~communications, from the point of view of assuring their security,~~  
~~was completed by the SSA and certain recommendations~~  
~~made to improve their security.~~

SECRET

reversal  
measures

~~SECRET~~

DRAFT

It is possible that for the State Department code room in Washington, and for such posts as have voluminous communications automatic, high speed, printing type converters M-325 could be provided by converting Sigaba machines. Such a conversion is practical and would in no way jeopardize Army or Navy cryptographic communications, since the converted machines would not disclose the principles underlying the Sigaba.

~~long as United States Army or Navy cryptographic security is not jeopardized.~~

6. In order to facilitate production of cryptographic systems, training of code clerks, maintenance of ~~the~~ equipment, and handling of traffic, it is desirable that the same basic <sup>mechanisms of</sup> cryptographic equipment be used throughout an organization. This is not the situation <sup>in</sup> of the State Department communications net at the present time, since both HCM and M-134-A cipher machines are now in use. The following three plans are offered as possible solutions to this problem:

a. The United States Army has available thirty (30) <sup>Converter Type</sup> M-134-A cipher machines. This equipment <sup>is obsolete so far as U.S. Army use is concerned and</sup> could be issued to the Military Attachés at an Embassy or Legation, <sup>as the case may be.</sup> <sup>its</sup> Military Attaché <sup>would</sup> be responsible for maintaining <sup>direct</sup> physical and cryptographic security. The equipment could be operated under his supervision by United States Army personnel which would be furnished <sup>the Ambassador or Minister</sup> ~~him~~ him for this purpose.

b. An alternate plan would be to <sup>make available a new U.S. Army device called</sup> issue the Converter M-325 for State Department use. <sup>This is a hand-operated device of high security but relatively low speed,</sup> The cryptographic principles involved in the <sup>device</sup> M-325 are similar to those of the German Enigma; however, the mechanical design of the M-325 is <sup>far</sup> ~~not~~ superior to the German design, and offers <sup>far greater possibilities for variation,</sup> It is felt that the M-325 could be <sup>provided for all</sup> ~~issued to present~~ State Department <sup>Embassies and Legations</sup> installations requiring high level cryptographic systems. It would be necessary to train <sup>State Department</sup> personnel at these installations in the <sup>use and</sup> maintenance of the equipment; however, it is quite simply constructed and <sup>relatively</sup> easy to maintain. Several hundred M-325 cipher devices <sup>could</sup> ~~can~~ be made available to the State Department <sup>for this purpose</sup> in the near future.

~~Their issue would be limited to Embassys and Legations.~~

The principal disadvantages of this plan are that (1) the equipment is obsolete (2) the M-325 is a hand-operated device and (3) the M-325 is not as secure as the Enigma.

Abstract from  
for [unclear]  
of [unclear]

Therefore making the machine far more secure than the Enigma.

Since rotors are frequently changed and the reversal rotor is changed daily, which is not possible in the Enigma, this

SECRET

want

Since this type is obsolete no more machines are being manufactured and therefore if it were <sup>desirable or</sup> necessary to extend the distribution within the State Department, none would be available. Even if no more were needed the matter of <sup>supplying</sup> replacement parts would present <sup>insurmountable</sup> difficulties. As the machines get older it would be increasingly difficult to maintain them and military personnel for this purpose and for their efficient operation would have to be provided on a more or less permanent basis.

\*\* it being approximately equal in this respect to the speed of the strip cipher device but of far greater security.

the State Department code room in Washington, London, and a very few additional

c. A composite plan embodying the principles of a and b, above,

would be to limit the issue of the <sup>Converter</sup> cipher device M-134-A to selected such as Madrid, Lisbon, Stockholm, Algiers, Cairo, Ankara, and Istanbul. Embassies, The selection would be accomplished through conferences

between representatives <sup>of</sup> from the War Department and ~~from~~ the State Department.

The provisions for maintaining cryptographic and physical security would

be the same as those outlined in a, above. All Embassies and Legations

could be <sup>provided with Converter</sup> authorized to hold cipher device M-325. This plan would provide high level, high speed cryptographic communications <sup>between the Department and</sup> for those Embassies

handling large amounts of traffic and would also provide a highly secure

but less rapid cryptographic device for State Department <sup>Communications between the Department and its smaller Embassies</sup> installations

and Legations having less heavy traffic loads. ~~\*\*\*~~ <sup>outlined in Part 6 C is</sup>

~~7. It is recommended that if <sup>the composite</sup> this plan is adopted the State Department be authorized <sup>Converter</sup> cipher device M-134-A for <sup>use at the</sup> issue to Embassies in Stockholm, Lisbon, and Madrid, and, as they desire, <sup>additional machines be issued for use at</sup> in Algiers, Cairo, Ankara, and Istanbul.~~

~~It is further recommended that authorization be <sup>obtained</sup> granted from Assistant Chief of Staff, Operation Division, to assign United States Army personnel to the Military Attaches <sup>STATE DEPT</sup> at ~~these~~ locations <sup>holding the cipher device M-134-A</sup> to operate and maintain ~~the~~ equipment.~~

**THE DUTIES OF SUCH PERSONNEL WOULD BE TO OPERATE AND MAINTAIN THE CRYPTOGRAPHIC EQUIPMENT.**

30  
8  
38

- Washington 8
- Stockholm 2
- Madrid 2
- Lisbon 2
- Helsinki 2
- Rome 2
- Berne 2
- Algiers 2
- Cairo 2
- Ankara 2
- Istanbul 2
- Paris 2

7. Of the foregoing three plans, the second appears to be the most advantageous, and authority for recommending it to the State Department for its consideration is requested. Details as to procurement, issue, use, etc., could then be discussed with the State Department.

\*\*\*Add to part c) b c  
 The disadvantages of this plan are that (1) the servicing and maintenance difficulties mentioned under plan a would still be present so far as concerns the M-134-A machines, (2) military operating and maintenance personnel would still have to be provided to a limited extent, <sup>and</sup> (3) the high-level communication devices would be of two different types, making intercommunication among all installations ~~of~~ more complicated.

If ~~the~~ plan b is adopted authority is required to procure the necessary additional Converters M-315 ~~for~~ to release the number required for State Department use from Army procurement and procure replacements therefor for Army use. Authority is also required to procure and transfer to the State Department the automatic Type M-315 machines and to divert sufficient Sigaba production to this purpose if they are to be received prior to the early part of 1945