

~~3~~
~~3~~
~~3~~
3 e

Declassified and approved for release by NSA on 09-19-2013 pursuant to E.O. 13526

IN REPLY
REFER TO

WAR DEPARTMENT

SPSIS-3

OCSigO.461 Codes
(4-10-42)OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

April 10, 1942

MEMORANDUM TO: Assistant Chief of Staff, G-2

Secret

By Authority of the
Chief Signal Officer

Initials

Date

676 4/10/42

1. Colonel Tiltman, Officer in Charge of the "Services Division" of the British Cryptographic and Cryptanalytic Service has presented details of and has requested our comments and criticisms on the cryptographic systems which they are now using and propose for future use in their field forces. Examination of these systems convinces us that they are very slow, complicated, and impracticable for our use in case our field forces had to work and communicate with British forces in joint operations. It is furthermore believed that the degree of security afforded by the British field systems is inferior to that afforded by either our present strip ciphers based upon Cipher Device M-138-A, or the proposed M-209 Device.

2. It is thought very desirable that we confer with Colonel Tiltman with respect to the possibility of their adopting our strip cipher systems as well as the M-209 Device, at least for joint use. It would be conducive to the security of our own forces when operating with the British to have them use the strip cipher system and the M-209 Device but with their own keys.

3. The M-138-A Device is already known to and is used by the Canadian Air Force in certain types of communication with our own Air Force. The M-209 Device is also known to the Canadian and the British Governments, since it is a device that was procurable commercially in limited quantities before its adoption by us for field use.

4. It is proposed, if possible, to work out with Colonel Tiltman the basis for joint cryptographic systems using the M-138-A and M-209 Devices so as to permit of expeditious intercommunication between American and British units working together. However, these systems would be in addition to cryptographic systems (using these same devices) which would be restricted in distribution to American units, and which would therefore not be readable by the British. The discussions would specifically be restricted to these systems and devices and would exclude any discussion of our electrical converters.

FOR DEFENSE

BUY
UNITED
STATES
SAVINGS
BONDS
AND STAMPS

SECRET

3115
 4-10-42

OCSigO. 461 Codes
(4-10-42)

SPSIS-3

5. The U. S. Navy has been consulted in regard to this proposal and is agreeable thereto.

6. Authority is requested to discuss in detail with Colonel Tiltman the possibility of establishing joint cryptographic systems of the category mentioned in paragraph 4.

For the Chief Signal Officer:



Frank E. Stoner,
Brigadier General, U.S. Army


MID 311.5 (4-10-42)

1st Ind.

G-2, W.D. G.S., War Department, Washington, D. C. APR 17 1942
To: Chief Signal Officer, War Department, Washington, D. C.

Authority is granted to discuss the possibility of establishing joint cryptographic systems using the M-138-A and M-209 Devices with Colonel Tiltman, Officer in Charge of the "Services Division" of the British Cryptographic and Cryptanalytic Service.

For the A. C. of S., G-2:



HAYES A. KRONER,
Colonel, General Staff,
Chief, Military Intelligence Service.

~~SECRET~~

Handwritten notes:
 looked over... request from
 Col Carter... do not
 Tiltman... which was
 done at Navy... and
 Col. Wenger...
 I was...
 maintain...
 256...
 W.D. G.S.