~~SECRET~~

~~SECRET~~

ARLINGTON HALL STATION

Date

TO ✓ FROM

- Commanding Officer
- Executive Officer
- Asst. Executive Officer
- Adjutant
- Asst. Adjutant
- Chief, Headquarters Branch
- Chief, A Branch
- Chief, B Branch
- Chief, C Branch
- Chief, D Branch
- Chief, E Branch
- Chief, F Branch
- Dir. of Com. Research ✓
- Dir. of Training
- C. O. of Troops
- Property Officer
- Personnel Officer
- Provost Marshal
- Classified Mail Room
- Secretary to C. O.
- File Room

- Comments & Return
- Recommendations
- Information
- Information & Return
- Inf. & Forwarding
- Your Inf. & File
- Signature, if approved
- See Note on Back
- As Requested
- As Discussed
- Your Action By

1. If the brief summary produced by G-2 is satisfactory, why can't the ONI summary also be made briefer?
2. This raises the question: Why are two summaries necessary? And why should not this

~~SECRET~~

State DRBE, IN 67328 primarily responsible for its own Comm. security, get out one summary for both services?

3. For greatest protection after the end of hostilities, I think it would be a good idea to have in reserve a complete change for every system (including those of State Dept.) so that immediately armistice comes, entirely new keys will go into effect almost automatically — & summaries stopped.

4. As an immediate step, however, I concur in PS of May. Hiss's rec.

J.

~~SECRET~~

23 June 1943.

MEMORANDUM FOR COLONEL CLARKE.

Subject: Navy distribution of State Department material.

Whether or not the Navy should furnish a summary of State Department dispatches to the British can not be positively answered by the S.S.S. It seems to me, however, that if State Department information is to be disseminated, it should be done by the State Department and not by the Navy or the Army.

The S.S.S. has for some time served as advisor to the State Department on cryptographic security. Many of their cryptographic systems were prepared by the S.S.S. or in consultation with us. At present the State Department is using cryptographic systems with a reasonable degree of security. However, it is not unlikely that many of them can be read if an enemy nation should make every effort to do so. Of course, any of the systems are susceptible to physical compromise.

Assuming it is desirable that the British be furnished the information in our State Department dispatches, it would always be possible to change the systems promptly should it be decided to no longer publish the dispatches. This would provide some immediate security, but it cannot be denied that by this time the British could have gained a considerable knowledge of our systems and our method of use.

For greatest protection after the end of hostilities, I think it would be a good idea to have in reserve a complete change for every system used by the State Department so that immediately armistice comes entirely new keys will go into effect almost automatically. At that same time undoubtedly summaries will be stopped.

As a solution to the immediate problem, it is suggested that the form of the daily summary be changed to a digest in which all references to dates, message numbers, etc. would be eliminated. All messages should be completely paraphrased with all quotes removed. This would increase the difficulty of using paraphrases as "cribs" and would offer a middle course causing the least amount of embarrassment to all concerned.

SIS
Date: 23 June Sig. W.P.C.

W. Preston Corderman,
Colonel, Signal Corps,
Commanding.

~~SECRET~~

SECRET

ROUTING AND WORK SHEET

(PAR 70.62 O.R.)

~~Secret~~
By Authority of the Chief Signal Officer
Initials RMB Date 14 June 43

SUBJECT ONI "Brief of Telegrams of Department of State"

NUMBER EACH ACTION	TO	MEMORANDUM	NAME, DIVISION OR BRANCH, AND DATE
1	Colonel Corderman	1. The problem as to whether the Navy should furnish a summary of State Department despatches to the British is one which cannot be positively answered by this office. No need can be seen for furnishing this information, however, it is possible there is a valid reason. 2. The State Department is using cryptographic systems with a reasonable degree of security. Most messages handled on the Washington-London circuit are cryptographed in a system which is highly secure from cryptanalytic attack. Most other State Department holders use cryptographic systems which are reasonably secure although not of the order of the London-Washington circuit. The general quality of the State Department systems has improved immeasurably since the beginning of the war. All State Department installations in the class of embassies, legations, plus some councils hold strip or machine systems for handling secret traffic. Further, all secret traffic is handled in a machine or strip system. 3. It is entirely true that paraphrases of messages would be of great value in breaking into a cryptographic system, and this case is no exception. It is entirely possible that given sufficient "crib" (which these paraphrases could well be), the daily keys for the generally held strip system could be recovered. It is not believed the system used on the London-Washington circuit could be broken cryptanalytically in this manner. Of course, any of the systems are susceptable to physical compromise. 4. Assuming it is desirable that the British be furnished the information in our State Department despatches, there should be no great concern over the se-	

SECRET

ROUTING AND WORK SHEET

(PAR 40.62 O.R.)

SUBJECT ONI "Brief of Telegrams of Department of State"

(Cont'd)

NUMBER EACH ACTION	TO	MEMORANDUM	NAME, DIVISION OR BRANCH, AND DATE
1 (Cont'd)		curity of the cryptographic systems with respect to the British providing these systems can be changed immediately should it be decided to no longer publish the despatches. The systems in use in the State Department could be easily changed providing sufficient time were given for the distribution of new keys.	
		5. As a recommended solution to the problem, the form of the daily summary might be changed to a digest in which all references to dates, message numbers, etc., would be eliminated. All messages should be thoroughly paraphrased with all quotes removed. This would greatly increase the difficulty of using paraphrases as a "crib" and would offer a middle course causing the least amount of embarrassment to those concerned.	
		Attached: #1 Memo for Col Clarke dtd 15 June 1943 #2 Memo for Col Clarke Dtd 11 May 1943 w/ Encls. A & B #3 Buck Slip frm Col Clarke #4 Buck Slip frm Col Corderman	CHH Charles H. Hiser Major, Signal Corps Cryptographic Branch 19 June 1943