New code being built - should have ~~DSI~~ gp
Vertical, pt to pt
system, for 134
to 11v

Salmon —
11 AM Saturday

~~SECRET~~

DRAFT 2 December 1943

REPORT ON STUDY OF CRYPTOGRAPHIC SYSTEMS USED BY STATE DEPARTMENT

1. In accordance with memorandum from Colonel Corderman dated 29 November 1943, subject "Resurvey of State Department Security" a committee consisting of Major Brown, Captain Douglas, and Captain Moak called upon Mr. Salmon 1 December 1943. All systems currently used by the Department were studied from a purely technical point of view. This report does not consider actual use of the systems by operating agencies nor the questions of physical security.

2. Six basic systems are in use by the Department: Cipher device M-134A, cipher device CSP 1127, strip systems, A, B and C enciphered code systems, BROWN code, and GRAY code. The findings of the committee with regard to each system are as follows:

a. Cipher device M134A - The committee is of the opinion that this device provides a maximum of cryptographic security and that it is being used in an approved manner.

b. Cipher device CSP 1127 - The committee feels that this device also provides a maximum of cryptographic security and that it is being used in an approved manner.

c. Strip systems - The committee recommends the following changes in the construction and use of these systems:

(1) Each vertical system should consist of a different alphabet set and key list.

(2) A daily word count of traffic in each system should be compiled in order that system changes may be effected with more accuracy.

d. A, B and C systems - The committee feels that these systems do not provide the ultimate in security, however, the following changes are recommended pending the installation of more secure systems:

(1) That instructions for the use of these systems be amended to permit encipherment of succeeding indicators at any one of the four positions on each page.

(2) That each table be used for the encipherment of any number of groups from 15 to 35 inclusive.

(3) That a word count be kept on the use of each table so that changes may be made with the proper frequency.

e. BROWN and GRAY - These unenciphered codes are used for restricted traffic only and it is considered that they are adequate for this purpose.

3. It is recommended that the Department consider the use of one-time pads for SECRET and CONFIDENTIAL vertical communications, particularly at important stations such as Stockholm where electrical cipher machines are not available. The Department does not now possess the necessary facilities for the production of such pads but it is believed that any expense for the necessary equipment and personnel would be justified by the attainment of absolute cryptographic security.

~~SECRET~~