Department State

SECRET

ENCLOSURE A

SUMMARY REPORT OF COMMITTEE APPOINTED TO RESURVEY CRYPTOGRAPHIC SYSTEMS EMPLOYED BY THE DEPARTMENT OF STATE

I. PRELIMINARY.

1. In 1941, pursuant to a request of the Secretary of State, an interdepartmental committee made a survey of the cryptographic systems and associated procedures employed by the Department of State and made certain recommendations with a view toward their improvement as regards security.

2. Pursuant to a more recent request of the Secretary of State (letter of 23 November 1943), a resurvey of the cryptographic systems and of the methods used for the preservation of the secrecy of its highly confidential communications was made by the present committee which was appointed by the Chief of the Signal Security Agency in accordance with a directive of the Chief Signal Officer.

3. The present report is a summary of the detailed report of the findings and recommendations of the Committee. The detailed report is attached hereto as Enclosure B.

II. SUMMARY OF FINDINGS.

4. Although the recommendations of the 1941 Committee referred to in paragraph 1 above have been instituted to a considerable degree, certain important measures recommended by that Committee have not been carried out to the degree necessary to accomplish the desired results, and certain other measures have not been instituted at all or to only a partial degree.

5a. The cryptographic systems employed by the Department of State for communications classified as SECRET are technically sound and could yield the requisite degree of security if properly used. However, certain of the methods and procedures which are associated therewith and which necessarily have an important influence upon the security of the systems themselves are defective in some details.

b. As regards the systems employed for communications classified as CONFIDENTIAL, the Committee finds that these are defective to a degree sufficient to raise doubts as to their present security.

SECRET

X-REFERENCE FILED IN:
1. #847
2.
3.

1-14

g. The principal steps which are of an immediate character and which could ameliorate the possibly dangerous condition now existing in certain of these systems are briefly indicated in paragraph 9 below, and set forth in detail in Section III of Enclosure B.

6a. The Department of State is not self-sufficient in regard to the production and correct use of its cryptographic systems and relies upon the Navy Department and the War Department for certain of its operations in connection with the production of cryptographic material and for technical advice in its correct usage.

b. The space, facilities, and personnel available for the preparation and frequent revision, distribution, and accounting of its cryptographic systems, as well as for the establishment and maintenance of cryptographic security on a continuing and effective basis, are not adequate for the secret and confidential communications of the Department of State.

c. The Department has not been able to take full advantage of the possibilities afforded by the use of cryptographic machines. Such machines would greatly enhance cryptographic security and at the same time speed up the communications of the Department if employed on a wider scale.

7a. The physical security of the State Department Code Center appears adequate. Obviously, the Committee did not and could not investigate the physical security of code rooms in the embassies, legations and consulates abroad. However, information tendered the Committee tends to support the belief that in many posts physical security is inadequate.

b. The Committee could not investigate the manner in which literal-text versions of secret or confidential messages are prepared reproduced, distributed, handled, and filed within the divisions and subdivisions of the Department itself, nor of those of the large embassies and legations. Just what an investigation of the facts in these matters would disclose cannot be stated but the findings might have an important influence upon the problem of cryptographic security of the Department's Communications as a whole.

c. Within the Department itself a relatively wide distribution is made of the texts of secret and of confidential messages, the copies being produced by uncontrolled mimeograph process. The copies are not registered nor accounted for by the register numbers.

a. No specialized or formal training in cryptography or in cryptographic security is given the personnel assigned to cryptographic duties either in the Department or in posts abroad.

b. Because of limitations in the current salary scale, no careful initial selection of the personnel assigned to cryptographic duties in the code rooms, both in Washington and in stations abroad is possible. Nor can the services of competent personnel be retained for the length of time necessary for the training and experience of personnel required for the preservation of security of communication.

III. SUMMARY OF RECOMMENDATIONS.

9. The Committee recommends:

a. That the principal steps of an immediate remedial character indicated in Section III of Enclosure B be taken without delay.

b. That provision be made for the additional space, facilities, and personnel required for the preparation and for a much more frequent revision, reproduction and distribution of the cryptographic systems employed by the Department of State. The Department should either be made wholly self-sufficient in this respect, capable of performing all necessary operations on a sufficiently adequate scale to permit of the necessarily frequent changes in the materials involved, or else these materials should be provided the Department by some other qualified agency. The State Department should make wider use of modern cryptographic machines and should have machines designed specifically for its own usage. These should be developed by or for the Department.

c. That provision be made for the establishment of a reasonably large Cryptographic Security Group, staffed with competent cryptanalytic and associated clerical personnel, whose duties would be exclusively (1) to conduct research and studies, on a continuing and extensive basis, on the cryptographic systems used by the Department and especially on the thoroughness with which regulations for the proper employment of those systems are observed; (2) to establish and to conduct special training courses for the proper instruction and indoctrination of the code clerks employed by the Department, both at home and abroad.

SECRET

d.(1) That the Assistant Security Officer of the Department be designated as Cryptographic Security Officer of the Department of State; that he be placed in charge of the Cryptographic Security Group mentioned in subparagraph 9c; and that he be given sufficient authority (1) to check all incoming and outgoing messages, as well as all procedures associated therewith, from the point of view of cryptographic security, and (2) to report violations of cryptographic security to higher authority for immediate disciplinary action.

(2) That at each post abroad a commissioned Foreign Service Officer thereat be designated as Cryptographic Security Officer of the Station, who would be constantly on the lookout for violations of cryptographic as well as of physical security and who would have authority to report such violations through channels to the Cryptographic Security Officer of the Department of State in Washington.

e. That the Security Officer of the Department of State, upon the recommendations of the Cryptographic Security Officer, take all necessary measures for the enforcement of the regulations for the maintenance of cryptographic security in a manner that will either insure conformity thereto or else cause disciplinary action to be taken, including the infliction of severe penalties, for infractions thereof.

f. That the following recommendations of the 1941 Committee be executed or carried out to a greater degree than has hitherto been the case: 7b(1)(d); 7b(3); 7d(1); 7f(1) and (2); 7g; 7h(1) and (3).

William F. Friedman
William F. Friedman
Director of Communications Research

Robert D. Brown
Robert D. Brown
Major, Signal Corps

James U. Noak
James U. Noak
Captain, Signal Corps

James H. Douglas
James H. Douglas
Captain, Signal Corps

Arlington Hall Station
14 January 1944

SECRET

SECRET

ENCLOSURE B

DETAILED REPORT OF COMMITTEE APPOINTED TO RESURVEY CRYPTOGRAPHIC SYSTEMS EMPLOYED BY THE DEPARTMENT OF STATE

I. PRELIMINARY.

1. In accordance with the request of the Secretary of State (letter to the Secretary of War, 23 November 1943), the Signal Security Agency has made a resurvey of the cryptographic systems and methods of classified communication employed by the Department of State.

2. An original committee consisting of Mr. William F. Friedman, Director of Communications Research, Major Charles H. Hiser, and Captain J. G. Moak, all of the Signal Security Agency, was appointed by Colonel Corderman, Chief of the SSA, to conduct the resurvey. This committee met with Mr. D. A. Salmon and Mr. P. E. Goldsberry of the State Department 18 November 1943. At this meeting it was decided to appoint a working committee to make the actual report and draft any necessary recommendations.

3. At a conference held 30 November 1943 between Mr. Friedman, Major Brown, and Captain Moak it was decided that Major Brown, Captain Douglas, and Captain Moak would form the working committee.

4. The working committee called upon Mr. Salmon 1 December 1943 and made a study of all cryptographic systems employed by the Department. On December 3 the committee, with Mr. Friedman, called upon Dr. Geist, Chief of the Division of Communications and Records, and made arrangements to study the cryptographic procedures employed within the Department's code-room. The committee worked in the code room 16 December, and again 18 December when it completed its study.

5. The committee wishes to express its appreciation to Mr. Salmon, Dr. Geist, Mr. Goldsberry, Mr. Meyer, Mr. Taylor, and Mr. Parker and many other members of the Department, all of whom were most helpful to the members of the committee in carrying out their assignment.

SECRET

II. FINDINGS.

6a. The basic systems in use by the Department are classifiable as follows:

(1) Three high-grade basic systems, two involving the use of automatic cipher machines, and one involving the use of a hand-operated cipher device. These are employed for SECRET communications and are as follows:

(a) Cipher Machine MC (U.S. Army Converter M-134-A);

(b) Cipher Machine MCA (U.S. Navy MCM, Mark I, Short Title CSP 1127);

(c) Strip Ciphers (U.S. Army Cipher Device M-138-A).

(2) One medium-grade basic system using "A", "B", and "C" codes, superenciphered by means of cipher tables. These codes are employed for CONFIDENTIAL communications.

(3) One low-grade basic system using "Brown" and "Gray" codes, unenciphered. These codes are employed for RESTRICTED communications.

b. The findings of the committee with regard to each of the systems and the procedures relating to their use are set forth in paragraphs 7, 8, 9, and 10 below.

7a. As regards the secret or high-grade basic systems:

(1) The Department produces and distributes key lists and tables of daily settings for Cipher Machine MC. Operating and keying instructions issued by the Department are based upon those prepared by the Army for use with the Converter M-134-A. At present Washington and London are the only holders of this device. It is used for SECRET traffic between these points. The daily traffic load averages about 3000 to 4000 groups per day. A separate set of rotors is used for the traffic of agencies whose communications must pass through the State Department. A new set of rotors is being prepared to replace present State Department rotors in the near future. The device

is operated according to instructions, except that cases were observed wherein the operator selected as a new rotor alignment the rotor alignment appearing on the rotors at the completion of a previous message or part of a message.

(2) The Department produces and distributes key lists and tables of daily settings for Cipher Machine MCA. Operating and keying instructions based upon those prepared by the Navy are issued to all holders of the device. There are 10 holders of this device and, since all hold the same system, vertical and lateral communication is possible. The device is used for SECRET traffic only and the traffic load runs from 3000 to 10,000 groups per day. The device is operated in accordance with instructions, except that bona fide words instead of random groups of letters are selected for the initial alignment. Frequently, for messages of several parts, the message indicators are selected from complete sentences such as "Mary had a little lamb." These are divided into 5 letter groups and used in order, as indicators. The indicators are enciphered and do not appear in the message in clear.

(3) The rotor-assembly tables and key lists for both of the foregoing machine systems are now produced and issued on a yearly basis, that is, while separate cipher keys are provided for each day of the year, the entire list of 365 keys is prepared and issued in a single document. This practice is not as safe, from the standpoint of physical security, as preparing and issuing key lists on a monthly basis.

(4) The number of stations equipped with high-grade cipher machines is relatively small and it is felt that the Department is not taking full advantage of the excellent possibilities afforded by the use of such machines, which could greatly enhance the security and speed of the Department's communications. Moreover, a machine designed specifically for its use would be advisable but thus far the Department relies upon the Army and the Navy for such machines.

b. As regards Cipher Device M-138-A, the strip-cipher systems:

(1) The key lists and instructions for use with strip ciphers are produced and distributed by the Department. The mixed sequences for the alphabet strips are

made up and typed in format by the Department. They are then photographed by the Navy Department, the actual strips being produced by the Signal Security Agency of the Signal Corps. The same key list is in simultaneous use by as many as fourteen holders; however, different sets of strips are supplied to each individual holder. Key lists are prepared and issued for a 12 months' period and consist of 40 keys per list, so that keys are used several times, although the strips change monthly for all systems.

(2) Some systems use what is termed a "straight board", that is, the cipher text for one set-up of 30 letters is taken from one column only; other systems use what is called a "split board" in which the first 15 cipher letters are taken from one column and the second 15 letters are taken from a different column, while still other systems use channel elimination, in which 5 different strips are eliminated from the board for each message or part. The instructions clearly state that the generatrices will be picked at random; however, numerous instances were found in both incoming and outgoing messages where no such random selection of generatrices had been made, resulting in numerous unnecessary and dangerous repetitions of some generatrices. (See attached graphs, Tab A).

(3) What has been stated under a(3) above as regards preparation and issue of keys for the machine-cipher systems is equally applicable to the strip-cipher systems.

c. The committee deems the three above-mentioned high-grade basic systems to be technically sound. If properly used they could yield the requisite degree of security for the secret communications of the Department. However, certain faulty details in methods and procedures associated with these systems, as noted above, should be corrected.

8. The medium-grade systems:

a. Three basic code books are used; "A", "B", and "C", published in 1919, 1922, and 1927, respectively. The codes are of two-part construction, composed of code groups with only a one-letter difference. The codes have been in effect since shortly after publication. Prior to July 1942

the codes were enciphered by means of digraphic tables. Since that time monographic tables composed of 10 pages of 20 alphabets per page have been used.

b. While instructions for the use of these tables require that not more than 32 groups be enciphered on the same page, numerous instances were found in which this figure was exceeded. Instructions require that the cipher indicators be enciphered only in the last position of the page. Also, it was found that the basic books in this system contained only 50 cipher indicators each, allowing insufficient variants.

c. The committee feels that in view of their long usage the basic codes (A, B, and C) must be considered compromised and that the cryptographic system for superenciphering messages in those codes does not yield adequate security for a voluminous number of confidential messages.

9. As regards the low-grade basic systems, the BROWN and GRAY codes are two-part codes; BROWN has been in effect since 1938 and GRAY since 1918. There is positive evidence to indicate that both of these codes have been compromised and that the Axis Powers have been deriving useful intelligence from the reading of messages in these codes. The committee considers that these codes are not adequate for use in war-time even for restricted traffic.

10. Investigation with respect to general policy and procedures revealed the following:

a. Although the recommendations of the Survey Committee of 1941 have been followed to a considerable degree, certain important measures recommended by that Committee have not as yet been carried out to the degree necessary to accomplish the desired results, and certain other measures have not been instituted at all or to only a partial degree. In the latter two categories are the following (see Tab B); paragraphs 7b(1)(d); 7b(3); 7d(1); 7f(1) and (2); 7g; 7h(1) and (3).

b. Physical security of the code room in Washington appears adequate. The committee was informed that special agents of the Department have recently studied the matter and made certain recommendations for improvement therein. In this connection it should be stated that it is understood that in the necessary destruction of obsolete or defective classified

material, work sheets, carbon paper, etc., no adequate supervision is exercised by code room personnel to insure that all documents are actually burned and that the burning is complete.

g. The committee could not investigate the physical security of code rooms in the field but a State Department representative stated that his investigations in 1941 in South America revealed that physical security conditions there were generally lax. Other information available to the committee indicates that in many posts physical security is inadequate.

h. As regards the selection, investigation, qualifications, and training of personnel, the committee was informed that no definite standards have been set and followed by the Department in selecting personnel for the code room and that salaries and ratings are in some instances too low to attract capable and trustworthy personnel. It was noted that the Chief of the Division is making efforts to improve this situation. As regards cryptographic personnel in foreign stations, there have been instances where selection and assignment to code duties has not been preceded by careful investigation as to loyalty and integrity.

i. The committee noted that the security classification of the plain-text versions of messages did not appear conspicuously on the pages of these messages, although a stamped warning that the message must be paraphrased if passed on to a non-governmental agency appears on the message. A symbol indicating the basic system in which the message was enciphered appears on the plain-text version. This is a faulty practice.

j. Literal plain-text versions of classified and unregistered messages are reproduced by uncontrolled mimeographing and are given a fairly wide distribution within the Department. These copies are supposed to be returned to the DCR but are not accounted for by register number and the disposition of copies is not controlled.

k. A study of traffic by the committee and corroborative statements by the chief code clerk indicate that stereotypic beginnings and endings are prevalent. Some stations show individual initiative by burying the classification and address in the body of the message. It was also found that in many instances entire paragraphs of messages, and in some cases almost the entire message, were direct quotations of letters,

speeches, and newspaper articles. No evidence was found that these had been paraphrased before encipherment.

h. The cipher text and literal plain-text in all but MC and MCA messages appear together on the work sheets. Plain and cipher text versions in MC and MCA systems are stapled together. These work sheets are filed and held for a considerable period of time. Some of these work sheets observed by the committee had been on file for a year.

11g. The Department of State does not have facilities or personnel for studying its traffic with a view to finding weaknesses in its cryptographic messages and detecting violations of the rules for preserving cryptographic security. The committee wishes to emphasize a fact which has been discovered by all security groups which have had actual practical experience in these matters: Even the most technically sound cryptographic systems leave messages open to solution if the systems are not properly employed and constantly scrutinized in their actual usage. Only by constant vigilance and continued study of the traffic itself, regardless of theoretical considerations of unsolvability, can there be assurance that the systems are not being abused and that the messages are not open to solution by a well-organized enemy cryptanalytic staff. The Assistant Security Officer of the Department, who is in charge of the compilation of the Department's cryptographic systems does not have the staff necessary for such studies as the foregoing, and therefore cannot check incoming and outgoing messages and all procedures associated therewith from the point of view of cryptographic security. There do not appear to be any cryptographic security officers in posts abroad who make a study of the local use of codes and ciphers to insure security.

h. At present the Department does not have adequate training courses or programs for the instruction of its cryptographic personnel. For the most part such personnel are assigned to duty and learn as best they can, by "on-the-job" training. No formal training is given in security matters. With a single exception, the personnel of the code room in the Department have had no formal training in cryptography, cryptanalysis, or cryptographic security. Consequently, only the most flagrant violations of cryptographic security are recognized by code clerks or their supervisors.

i. Violations noted either in the Department or in posts abroad have not been followed by disciplinary action

of a severity sufficient to instill a fear of consequences for future repetition of violations.

III. RECOMMENDATIONS.

12. In order to obtain the maximum in cryptographic security for the Department of State, the committee submits in paragraphs 13, 14 and 15 recommendations of a specific nature for each type of system. In paragraph 16 it submits recommendations of a general nature.

13. Recommendations regarding machine systems:

a. Rotor assembly tables and settings should be issued on a monthly basis.

b. Standard, authorized instructions issued by the Department should be followed at all times in the selection of rotor alignments.

c. A random choice of internal indicators should be made by the operators.

d. For stations provided with cipher machines separate key lists should be provided for the handling of traffic of all three categories of messages, to expedite the handling of CONFIDENTIAL and RESTRICTED messages as well as SECRET.

14. Recommendations regarding strip systems:

a. All strip systems should be converted to channel elimination. It is understood that this is being done as expeditiously as possible.

b. Specific instructions should be issued to insure (1) that care is taken to use a given generatrix but once in the same part of messages enciphered in channel elimination systems, and (2) that in strip systems not employing channel elimination, cipher columns should be selected by the operator in such a way as to avoid certain columns being used more frequently than others.

c. Each holder of a strip system used for vertical communication should be provided with a unique key list.

d. Key lists should provide a different arrangement of strips for every day, but the present practice of changing strips every month for each system should be continued.

15. Recommendations regarding code-book systems:

a. The present systems using cipher tables for superenciphering code messages in the A, B, and C codes should be discontinued and replaced by "one-time pad" systems so far as practicable. Where subtractor tables for general intercommunication must be used, a safe indicator system must be employed in connection therewith.

b. The A, B, and C codes, if the systems employing such codes are retained, should be replaced by new editions. The code book now in preparation by the Department should include figure code groups as well as letter code groups, so that either numerical one-time pads or letter one-time pads could be used for encipherment of SECRET and CONFIDENTIAL messages where these systems must be used.

c. The use of BROWN and GRAY codes even for RESTRICTED traffic should be discontinued. The Committee feels that in war-time all traffic should be transmitted in secure systems.

16. Recommendations of a general nature applicable to all systems:

a. The Department should have a technically competent and adequately staffed cryptographic security group, under the Assistant Security Officer. The latter should be given the responsibility for making a continuing study and check of incoming and outgoing messages with regards to cryptographic security, for reporting violations of cryptographic security to high authority for immediate disciplinary action, and for recommending from time to time, as necessary, changes in the cryptographic systems employed by the Department and in the regulations covering the use of these systems.

b. Definite standards in selection of personnel should be set up by the Department and that present efforts to increase Civil Service ratings of personnel in the code room be continued.

c. Surveys should be made in all foreign stations with a view to providing adequate physical security at all such stations. It is further recommended that periodic checks be made at all stations to see that this security is maintained.

d. Cipher key lists should be prepared and issued on a monthly rather than on a yearly basis.

e. All classified messages circulated within or outside the Department should be conspicuously stamped with their classification, i.e., "SECRET", "CONFIDENTIAL", or "RESTRICTED", and that investigators of the Department study the handling and safeguarding of such messages.

f. The practice of indicating by specific symbol on the plain-text version of a message sent in cryptographic form the system in which the message was cryptographed should be discontinued.

g. Stereotypic beginnings and endings of messages should be eliminated. Direct quotations from newspaper articles, speeches, and letters should insofar as practicable be held to a minimum. In all enciphered messages where direct quotations are necessary, the committee recommends the use of one-time pads.

h. The plain and cryptographic text of a message should not be filed together at any time. To do so violates one of the fundamental rules of cryptographic security. It is recommended that plain and cryptographic text be filed separately and that the former be afforded the same protection as the original cryptographic system.

i. The destruction of all classified trash should be witnessed by responsible personnel of the code room. Care must be exercised to insure complete destruction of all such material.

17. Final recommendation: In view of the importance of maintaining indefinitely the security of messages handled by the Department of State the committee recommends that every effort be made by the Department's code section to attain maximum cryptographic security. It is believed that the ultimate objective of the Department should be to use high-grade cipher machines and one-time pads for the transmission of all classified messages and to insure that its cryptographic systems are properly employed. It is felt that the expense involved therein should not be considered. To follow the recommendations set forth above will require the addition of considerable personnel, material, and space but this is absolutely necessary if the security of Department of State communications is to be achieved and maintained.

~~SECRET~~

William F. Friedman
William F. Friedman
Director of Communications Research

Robert D. Brown
Robert D. Brown
Major, Signal Corps

James G. Noak
James G. Noak
Captain, Signal Corps

James H. Douglas
James H. Douglas
Captain, Signal Corps

Arlington Hall Station
14 January 1944