CONFIDENTIAL

REPORT OF SPECIAL COMMITTEE TO INVESTIGATE SECURITY OF STATE DEPARTMENT COMMUNICATIONS

1. In respective letters dated May 12, 1941, to the Secretary of the Navy, the Secretary of War, and the Director of the Federal Bureau of Investigation, the Secretary of State requested that representatives of those agencies be designated "to serve in an advisory and consultative capacity with officers of the Department of State" for the purpose of assisting the Department in making "a most careful survey of its codes and ciphers to determine their efficacy at this time and to discover and establish additional means of preserving the secrecy of its highly confidential communications under present world conditions." (Appendix 1.)

2. With these ends in view the following were designated:

Commander L. F. Safford, U.S.N. (Office of Naval Communications)

Captain H. G. Hayes, U.S.A. (Signal Corps, Office of the Chief Signal Officer)

Mr. W. G. Blackburn (Federal Bureau of Investigation)

Mr. Frederick Livesey (Department of State)

In addition to the foregoing, Mr. William F. Friedman, Principal Cryptanalyst, War Department, was designated to serve as Technical Advisor to Captain Hayes.

3. The Committee completed its investigation in four sessions, held on May 27, June 2, 9 and 12, 1941. Its findings and recommendations are embodied in this report.

CONFIDENTIAL

4. At its first session, May 27, a preliminary meeting was held in the office of Mr. G. Howland Shaw, Assistant Secretary of State, who discussed with the members of the Committee the nature and scope of the studies to be pursued by them and indicated that the Secretary of State desired the Committee to investigate all related phases of communication security in and for the Department.

5. The Committee then resumed its meeting in Mr. Salmon's office and after brief preliminary discussion agreed that its agenda embraced the following phases of communication security:

a. The technical soundness and the respective degrees of efficiency of the codes and ciphers now in use by the Department; and the related procedures and safeguards followed in their compilation or preparation, physical distribution, transportation, and accounting.

b. The facilities, procedures, and regulations for insuring the physical security of cryptographic paraphernalia both at the Department and at its offices in foreign countries.

c. The definitions and delimitations of classes of messages and documents with respect to the various degrees of confidentiality; and the regulations governing the drafting of messages to be transmitted in cryptographic form, as well as those pertaining to the placing of responsibility for determining and indicating the classification of messages.

d. The regulations governing the selection and proper

technical employment of the various authorized cryptographic systems in cryptographing messages; the regulations governing the preparation, handling, distribution and filing or ultimate disposition of plain-language versions of cryptographed messages; and the regulations governing the preparation of press releases dealing with matters which may have formed the subjects of cryptographic communication.

g. The principles followed in the selection, training and assignment to duty of personnel permitted to have access to cryptographic material or to perform cryptographic duties; and the principles followed in selecting the agencies of transmission employed in forwarding messages to their destination.

6. The details of the findings of the Committee in respect to the foregoing subjects of study are as follows:

a. (1) Although in general the several cryptographic systems now employed are technically sound and efficient, it appears that the various codes and ciphers could be distributed to holders according to a better defined and more orderly system.

(2) Although the methods used to superencipher messages prepared in certain systems are sufficiently secure, this is perhaps not true as regards certain other systems and it would

appear that the latter might not yield the degree of security desirable for the communications for which they are intended. The Committee is not in a position to submit a positive opinion in this respect because in order to do so a long and extensive cryptanalytic study would be essential.

(3) The methods and means used to encipher messages of highest secrecy and importance appear to be too slow for modern rapid communication and require more labor and personnel than would be the case if certain mechanico-electrical apparatus now available were employed for this purpose. Moreover such apparatus if technically sound can yield far greater cryptographic security than is possible with the present "hand-operated" means.

(4) The procedures and safeguards followed within the Department itself in the compilation and preparation of the codes and ciphers, and in their physical distribution and accounting appear to be satisfactory. However, registration of documents by "short titles" is not now the case and

~~CONFIDENTIAL~~

its establishment would be advisable. The Committee also feels that special forms for the receipt, destruction, semiannual accounting, and transfers of documents from one holder to another are quite necessary for an effective accounting system.

(5) As regards the methods followed in the transportation and forwarding of cryptographic publications and documents to authorized holders thereof, it is understood that such material is invariably carried by diplomatic courier, which should insure its safe delivery without possibility of compromise. However, special tests made by the Federal Bureau of Investigation of the security afforded by the various types of pouches employed for the purpose have demonstrated that it is easy to open and remove the contents of pouches, photograph and replace the original documents, and then resew the pouches so as to show no signs of tampering. The type of tumbler lock used on locked pouches offers hardly any guarantees of safety at all, since one of them

~~CONFIDENTIAL~~

was repeatedly "picked" successfully in a few minutes. The detailed findings of this study are embodied in Appendix 2.

h. Except at the Department itself and at only a few of the large embassies the facilities, procedures, and regulations for insuring the physical security of cryptographic paraphernalia appear to be woefully inadequate, these constituting in all probability the greatest source of danger to the security of all communications of the Department. Without adequate safeguards to preserve physical security of the cryptographic paraphernalia itself, no system for secret communication regardless of how sound it might be technically can be considered safe for use.

g. The Department does not appear to have clear-cut definitions of and delimitations for various classes of confidential matter; it does not appear to have clear-cut regulations governing the drafting of messages to be transmitted in cryptographic form; nor does it appear to place responsibility upon the proper persons as regards determining and indicating the classification according to which an outgoing message should be handled.

f. (1) In the absence of well-defined regulations governing the matters referred to in subparagraph g it is apparent that regulations governing the the selection of the specific cryptographic system cases cannot be applied properly or with certainty. ~~CONFIDENTIAL~~

(2) The regulations governing the technical employment of the various authorized systems appear to be adequate.

(3) The regulations and procedure governing the preparation, handling, distribution, and filing or ultimate disposition of plain-language versions of cryptographed messages, while satisfactory within the confines of the Communications and Records Division itself, appear to be woefully inadequate when these documents pass outside the aforementioned Division. It appears that an unspecified and constantly varying number of verbatim translations of incoming cryptographed messages must be prepared by DCR upon the request of officials of the Department who deem it necessary to furnish copies for the information of others who might be concerned. The reproduction of copies is now by means of uncontrolled mimeograph and this is regarded by the Committee as a highly dangerous practice. No accounting for the multiplicity of copies is made nor is there any assurance that additional copies are not made and circulated within the various divisions. Accounting for copies under these circumstances is not possible even with much more clerical

assistance than is now available. Further, there is neither uniformity nor certainty as to the manner in which these verbatim translations are handled or filed in the respective divisions to which they are sent, and in many cases doubt exists as to their ultimate disposition. While the Committee made no investigation as to the procedure followed in the case of outgoing messages initiated within the respective divisions, it would appear probable that there is considerable danger from the existence of work sheets and carbon paper bearing rough and final drafts of outgoing messages to be cryptographed in confidential codes and ciphers. Finally, it appears that no great care is exercised with regard to the number of persons to whom verbatim or even paraphrased copies of secret messages are shown, in many cases this being perhaps wholly unnecessary. These unsatisfactory conditions probably constitute the second great source of danger to security and, <u>if not corrected, security of communication can neither be maintained nor even established.</u> In this connection it is to be noted that in the military and the naval service a commissioned officer is

not, merely by virtue of his commission or his rank, entitled to receive secret information in which he is not directly and officially concerned.

(4) The Committee has reason to believe that there is no careful coordination between the persons having knowledge of the contents of cryptographed messages and those who prepare information embodied in the form of press releases which may contain matter transmitted or received in cryptographic form.

g. (1) Although the principles followed in the selection, training, and assignment to duty of cryptographic personnel within the Department itself appear to be satisfactory, the Committee has no knowledge of what may be the case in this regard in the Department's Embassies, Legations, and Consulates. It is true that the Department has specific regulations governing these matters, as embodied in Section VII-4 of its Foreign Service Regulations, but there appears to be no assurance that these regulations are scrupulously and uniformly observed at all stations. This appears to be a subject on which direct personal and periodic observation by properly trained inspectors would

be essential before definite assurance could be had as to the extent of conformity with pertinent regulations.

(2) It would appear that the Department avails itself of cable routes rather than radio channels wherever possible, a procedure which is to be highly commended. Further, the Committee understands that the practice of discussing confidential subjects over the transocean radiotelephone has been practically eliminated. The Committee desires to point out that despite assurances of "privacy" so often reiterated by the telephone company, such conversations are private only so far as the casual listener-in is concerned. They offer no obstacles to any person or organization having a real interest in learning the substance of such conversations.

7. The recommendations of the Committee are embodied below, but in order to present them in a well-integrated manner the successive recommendations do not follow the order in which the subjects and findings are treated in paragraphs 5 and 6 above. The Committee recommends:

a. That the Department of State adopt the same definitions of and delimitations for classes of messages

and documents (with respect to the various degrees of confidentiality, viz: RESTRICTED, CONFIDENTIAL, SECRET) that now subsist in the War Department and in the Navy Department (both of the latter now have identical classifications and practically identical definitions and delimitations therefor). These three classifications have been effective in those Departments for a number of years and have proved themselves technically sound and practicable. Furthermore, if the Department of State were to adopt the same classifications and definitions the three Departments would be well coordinated in this fundamental respect when intercommunication or the exchange of documents becomes necessary.

b. (1) That based upon the foregoing recommendation, the Department of State revise its present set up of cryptographic systems so as to provide adequate systems for cryptographic treatment of the three classes of messages in the following categories*:

(a) For communication between the Department and selected Embassies and Legations; and for intercommunication among them.

(b) For communication between the Department and all Embassies and Legations; and for intercommunication among them.

*Note: Each category should be provided with cryptographic paraphernalia belonging to all lower categories.

(c) For communication between the Department and selected Consulates; and for intercommunication among them.

(d) For communication between the Department and all Consulates; and for intercommunication among them.

(e) For communication between the Department and such Special Observers and Special Missions as may be found necessary.

(f) For communication between U.S. Naval Vessels and U.S. Embassies, Legations or Consulates.

(g) For such other special purposes as may be found desirable.

(2) That this distribution of cryptographic systems according to categories be accomplished by a suitable redistribution or reassignment of the present codes, so far as is possible, the codes to be provided with the same general system of superencipherment but operating with different cipher keys. For the latter purpose hand-operated methods employing cipher tables may be used, but it is possible that a cryptograph might be suited for the speedier superencipherment of certain types of confidential messages.

(3) That the Department establish a more detailed system of accounting for cryptographic paraphernalia, using special forms for receipt, semiannual report of possession, report of transfer from one holder to another, and report of destruction, these reports to be based upon "short titles" for all registered documents, devices or publications.

(4) The Department of State be provided with such literature and technical advice by the War and the Navy Departments as will be of assistance in the execution of this recommendation.

g. (1) That for its most secret communications the Department of State look seriously into the subject of automatic, electrically-operated cipher machines; and that the Department collaborate with the War Department or the Navy Department with a view to the introduction of suitable machines for use at the Department and at the largest and most important Embassies where speed and security of communication is essential under present world conditions.

(2) This recommendation, while entailing certain initial expenditures for machines, will ultimately result in some saving by virtue of a reduction

in cryptographic personnel, since one machine can do the work of several clerks.

(3) In this connection the Committee takes cognizance of the fact that negotiations with the foregoing end in view have been in progress between the Department of State and the War Department for some time and before the appointment of this Committee. It recommends, therefore, that these negotiations be concluded as promptly as practicable so that the machine may be placed in service without undue delay.

g. (1) That immediate measures be taken by the Department of State to provide suitable combination safes for the storage of cryptographic paraphernalia and and confidential files at all its Embassies, Legations, and Consulates not now provided with adequate facilities for proper safeguarding of these materials when not in use. Further, that the Department take immediate action to insure that only suitably paid American citizens are employed at outlying offices as guards when those offices are closed between office hours. On this crucial point reference is made to paragraph 6b.

(2) That instructions be issued to all offices requiring a complete change in the combinations to safes at least once a year and that these changes

be made by competent and duly authorized personnel in the office. (There is nothing about this matter which requires the services of "outside" experts; the application of ordinary common sense and careful study of the instructions which usually accompany such safes are adequate for the purpose.)

(3) In this connection the Committee takes note of the present requirement (Par. VII-4, Note 2(c) of Foreign Service Regulations) that "each time a change is effected in the combination of a safe the Department shall be informed by means of a card prepared in the following form..." and that "this card shall be transmitted to the Department in a sealed envelope...". The Committee doubts the necessity for this requirement and recommends its immediate elimination.

(4) That the Department of State collaborate with the Federal Bureau of Investigation in regard to the types of safes, cabinets, locked pouches, envelopes, etc., that should be employed for storage and transportation of cryptographic material.

g. (1) That the Department of State draw up new regulations governing the drafting of messages to

be transmitted in cryptographic form, basing them upon the new classification recommended in paragraph 7a.

(2) That responsibility for proper drafting, for proper classification and for clear indication of classification be placed upon the originators of messages; that the latter two decisions not be made a responsibility of the cryptographic personnel; and that the Department take such action as will insure observance of the regulations applicable to these functions.

(3) That new regulations governing the selection of the specific cryptographic system to be employed by cryptographic personnel be drawn up by the Department and that they be based upon principles that are technically sound, arising out of the recommendation contained in paragraph 7a.

(4) That the Department of State be provided with such literature and technical advice by the War and the Navy Departments as will be of assistance in the elaboration of the new regulations in point.

f. (1) That the Department draw up new and detailed regulations governing the preparation, handling, distribution, and filing or ultimate disposition of plain-language versions of cryptographed

messages for the guidance of all divisions within the Department and of all of its Embassies, Legations, and Consulates, these regulations to be based upon technically sound principles arising out of the adoption of the recommendation made in paragraph 7a.

(2) That these new regulations be rigidly and strictly enforced and that the Department take all necessary disciplinary measures to insure their strict enforcement by all concerned.

(3) That the Department be provided with such literature and technical advice by the War and the Navy Departments as will be of assistance in the elaboration of the new regulations in point.

g. That a tour of duty as coding officer at the Department in Washington or at an important office be made one of the mandatory requirements for the training and duties of junior career officers of the Foreign Service. These duties should correspond to those of coding officers in the Navy and should consist of the safeguarding of secret and confidential messages, plus routing, filing, distributing and paraphrasing messages; and advising superior officers as to correct procedure for the maintenance of communication security.

h. (1) That the Department take such measures as may be necessary to provide an adequate and technically informed inspection service for its cryptographic operations in foreign countries, with a view to insuring that all the regulations having a direct bearing upon communication security are observed.

(2) That the Department take steps to have designated at the Department in Washington and at each of its offices in foreign countries an officer who shall in addition to his other duties perform the duties of "cryptographic security officer", who will be responsible for the enforcement of all cryptographic and communication security regulations at his station.

(3) That the Department serve notice on all personnel concerned in the maintenance of communication security that severe disciplinary action will be taken in future cases of laxity, carelessness, or negligence in the observance of regulations established to preserve security.

~~CONFIDENTIAL~~

Leland P. Safford,
Commander, U.S.N.

Harold G. Hayes,
Captain, Signal Corps, U.S.A.

W. O. Blackburn

Frederick Livesey

William F. Friedman

APPENDIX 1:- Copy of letter from Secty of State to Secty of War, May 12, 1941

APPENDIX 2:- Findings of study of methods followed in transportation and forwarding of cryptographic publications and documents

June 26, 1941

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

COPY

DEPARTMENT OF STATE

May 12, 1941.

My dear Mr. Secretary:

The Department of State is desirous of having made a most careful survey of its codes and ciphers to determine their efficacy at this time and to discover and establish additional means of preserving the secrecy of its highly confidential communications under present world conditions.

I wish to enlist the aid of the War Department in the conduct of the survey contemplated and I hope you may be in a position to designate a qualified commissioned officer of the War Department to serve in an advisory and a consultative capacity with officers of the Department of State, the Navy Department, and the Federal Bureau of Investigation for these purposes, the importance of which I believe I need not emphasize.

Your cooperation will be very much appreciated.

Sincerely yours,

/s/ Cordell Hull

The Honorable

Henry L. Stimson

Secretary of War

APPENDIX 1

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Appendix 2

Specimens of each of the three types of diplomatic pouches and a specimen of sealed envelopes used by the Department of State were submitted to the Technical Laboratory of the Federal Bureau of Investigation for the purpose of determining the security of these items for the shipment of secret material.

Both the leather courier's bag and the large canvas diplomatic mail pouch make use of a Yale "Super-pin" tumbler padlock for sealing the pouches. In the Laboratory of the Federal Bureau of Investigation it was possible to successfully pick this lock a number of times, the time required varying from fifteen minutes to three hours. Inasmuch as it was possible to enter the leather courier's bag by removal of the lock in this manner no other attempt was made to enter the pouch.

In respect to the large canvas mail pouch, in addition to being able to enter this pouch by picking the padlock, it was also possible to enter it by means of removing the seam stitching and then replacing the stitches in the same manner as they were prior to removal. The time required to enter this pouch depends upon the number of rows of stitching it is necessary to remove, allowing approximately twenty minutes per row of stitching.

The canvas Air Mail pouch which was sealed with lead seals was entered by means of removing the seam stitching a

sufficient distance to allow removal of the contents, after which the stitching was replaced in the same condition as it was originally. This whole operation required approximately one hour.

The special Evilock envelopes which were sealed one within the other were entered by removing the seals and loosening the gum. These envelopes could then be refastened and sealed, the time required for the entire process being approximately one and one half hours including the reproduction of the seals. In this connection it is noted that the purpose of the locking feature is defeated to a great extent by placing the wax seal over the brass portion. It is possible to pry this locking device open, but of course in doing so a certain amount of damage is done to the brass. When this brass is covered by a wax seal, the replacement of a seal over the brass makes it impossible to determine that the brass lock has been tampered with.

This information is being given for the purpose of indicating the relative insecurity of these methods of transmitting secret material when it might be required to pass through any examining station equipped to this type of work.