16 July 1953

~~SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR MR. FRANK C. NASH

SUBJECT: Proposed NSC Directive for Communications Security

1. The Department of Defense members of the COMSEC Ad Hoc Committee agree that most of the directive, as drafted on 3 July 1953, is practical and workable and with some minor revisions will constitute an adequate foundation for organizing and conducting the U. S. COMSEC effort, in accordance with the Presidential Memorandum, on a national scale. However, there are a few points which, in the interests of conveying the intent of the NSC and general clarity, should be recorded. It is agreed that the intent of the President's Memorandum of 24 October 1952 is to take the steps necessary to establish, within the limits of practicability, a single technical agency empowered to act for the government in the field of COMSEC and a policy-making board to guide this technical agency and to ensure the cooperation of the executive departments. This draft accomplishes this initial and basic task quite well and needs only some final touching up to become a finished and usable instrument.

2. Specifically, it is recommended that the changes as shown in the inclosure hereto be made in the 3 July 1953 draft of the NSC Directive.

Incl:
Department of Defense Changes
to Proposed NSC Directive on
COMSEC, 16 July 1953

~~SECRET~~

~~SECRET - SECURITY INFORMATION~~ 16 July 1953

DEPARTMENT OF DEFENSE CHANGES TO PROPOSED NSC DIRECTIVE ON COMSEC

1. On page 7, line 15 - In paragraph 2 b - after the phrase, "departments and agencies of the government" add "and to adjudicate disputes arising from decisions of the Director, NSA".

Reason - Insertion of this phrase provides the departments and agencies with additional protection by providing a means for appealing technical decisions of the Director, NSA.

2. On page 3, lines 9 and 16 - In paragraphs 2 c (1)(a) and (b) respectively - delete the phrase "Subject to review by the Board in the event of disagreement".

Reason - The appeal procedure given in paragraphs 1 g and 1 h on pages 5 and 6 together with the change given above makes this phrase unnecessary now.

3. On page 3, lines 10 and 17 - In paragraphs 2 c (1)(a) and (b) insert the word "Prescribe" at the beginning

Reason - Cryptosecurity requires strong cryptoprinciple and proper procedures for their use. Determination of strong cryptoprinciples and procedures requires thorough and continuous cryptanalysis and utilizes lessons learned from study of foreign communications This can be done effectively and economically only by centralizing both the study of foreign communications and the authority to determine cryptoprinciples and procedures in one organization Centralized and absolute control over the cryptoprinciples incorporated or to be incorporated in equipment or cryptosystems is essential to assuring the adequacy of cryptographic systems and high and uniform standards of communication security as directed by the President This control involves (1) prescribing principles and procedures for new equipments and systems; (2) prescribing technical improvements when existing equipments and systems are found to be weak; (3) reviewing and approving all existing equipments and systems to insure the soundness of the principles and procedures used Prescriptive authority is necessary to exercise this control. Without it there is no means of preventing a department from using a weak principle which could be solved by an enemy and lead to the solution of stronger principles used by other departments.

4 On page 9, line 6 - paragraph 2 c (1)(d) - Reword paragraph as follows: "Under policies promulgated by the Board and subject to the exception granted the Director, Central Intelligence Agency under NSCID No. 5, conduct and coordinate the conduct of liaison on technical COMSEC and related matters with the cryptologic agencies of foreign nations and international organizations".

Reason - This clarifies the "technical" nature of the liaison over which NSA should have cognizance and should conduct under Board policies. Further close, working level liaison is essential to obtain maximum economy and efficiency

in providing and exchanging COMSEC materials involved in protecting US-UK and NATO communications.

5 On page 9, line 13 - paragraph 2 c (1)(e) - substitute the word "Board" for the words, "respective departments and agencies" and in line 16 substitute words, "the departments and agencies" for the word, "them".

Reason - The Director, NSA is guided primarily by the policies of the Board. It would be impractical and confusing for him to attempt to operate under the numerous and probably conflicting policies of the various departments. Since, previously, the Director, NSA has provided technical information and the departments have done the actual training of operating personnel, this change makes the paragraph consistent with practice and with the rest of the directive.

6. On page 10, line 2 - paragraph 2 c (1)(g) - delete phrase "subject to approval by the Board".

Reason - Approval authority over long-range plans for COMSEC is vested in the Board in paragraph 1 e (4) on page 5. It is not considered an appropriate assignment of responsibilities and authorities to require the USCSB to review continuously the details of the implementation of plans previously approved by it.

7. On page 10, line 5 - paragraph 2 c (1)(g) - delete phrase "consisting of projects of common concern which can be more efficiently accomplished centrally" on page 10, line 9 delete phrase "and coordination with" and insert "approval by"

Reason - In order to encourage the generation of ideas having potential COMSEC value and to assure their early and effective exploitation, authority and responsibility for COMSEC research and development should be centralized, and active participation by all COMSEC users should be encouraged. The organization responsible for prescribing cryptoprinciples and cryptosecurity procedures should be assigned cognizance over the national COMSEC research and development program in order to assure effective utilization of the limited research and development personnel and facilities of the various departments and agencies. It should not be restricted to "projects of common concern" if the overall COMSEC program is to be effective in assuring a satisfactory state of security. For efficiency and economy it is essential to national security that the government maintain continuously an integrated COMSEC research and development program, rather than merely "review and coordinate" a diversity of such programs.

8. On page 10, line 14 - paragraph 2 c (1)(h) - Delete the phrase "insofar as practicable" and in line 15 - after the words, "the compatibility" and the words, "and insofar as practicable, the standardization".

Reason - The compatibility of crypto-equipments is essential to intercommunication. Although different conditions call for different shapes and construction, crypto-equipments designed for the same general communication purpose must be able to work together. Standardization of techniques, parts, and materials to the greatest extent possible consistent with the intended application of the equipment will help reduce costs and will simplify usage.

9. On page 11, line 3 - paragraph 2 c (1)(i) - Delete the words "only on a reimbursable basis" and substitute the words "on a fiscal arrangement as mutually agreed with the departments and agencies".

Reason - The provision of COMSEC materials and technical assistance to the departments and agencies is a basic service of the Director, NSA. In order to be able to provide this service in the simplest, most direct, and satisfactory manner possible, the specific financial arrangements should be flexible as far as this directive is concerned. The change proposed opens the way for different but mutually satisfactory arrangements between the Director, NSA and any individual department or agency.

10. On page 11 - Add new paragraph 2 c (1)(j) to read "The Director, NSA is responsible for insuring adequate capacity for and providing technical criteria for producing cryptomaterial to meet legitimate requirements. Nothing in this directive shall be construed as precluding the Director, NSA from producing, printing, procuring, and modifying cryptomaterials to meet the requirements of the departments and agencies or from budgeting for the conduct of his activities".

Reason - The President's Memorandum requires the satisfaction of legitimate requirements. In order to assure that there are operating facilities and technical criteria adequate to do this and to be better prepared to meet the demands of a mobilization it is essential that the Director, NSA be specifically authorized to engage in these activities. The present cryptomaterial production facilities including special and unique machinery and a staff trained and skilled in its use must be kept in operation for the security of the nation.

~~CONFIDENTIAL - SECURITY INFORMATION~~

MEMORANDUM FOR MR. FRANK MASH, OSD

SUBJECT: NSC Directive on COMSEC

1. It is the considered opinion of the undersigned that paragraph 2a of the extant draft establishes an arrangement which should be avoided by the Secretary of Defense and consequently should be objected to.

2. In the COMINT directive the Department of Defense is made Executive Agent of the Government. This draft proposes the Department of Defense as Executive Agent of the United States Communications Security Board.

3. This, it seems to me, creates a paradox in that the Secretary of Defense as titular head of the Executive Agent becomes subordinate to the Board, an organization which in turn is subordinate to him as a member of the Special Committee, and which in its membership, includes one of his own subordinates. Thus we find the Secretary subordinate to a subordinate to himself.

4. In order that uniformity of organization between COMINT and COMSEC may be maintained without confusion and to establish the Secretary of Defense on the same level as the Board with respect to the Special Committee, it appears most desirable to retain and utilize in this COMSEC directive the same relationship as used in the COMINT directive, i.e.: The Department of Defense is designated as executive agent of the government for all communication security matters.

Respectfully,

ALFRED R. MARCY
Colonel, US Army
Deputy Director