~~SECRET~~ ~~SECURITY INFORMATION~~

16 July 1953

~~SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE EXECUTIVE SECRETARY, PLANNING BOARD,
NATIONAL SECURITY COUNCIL

SUBJECT: Proposed NSC Directive for Communications Security

Forwarded herewith are the specific changes to the proposed NSC Directive on communications security which are considered necessary.

ALFRED R. MAHAN
Colonel, US Army
Deputy Director

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

Copy of letter to Secretary Wilson

~~SECRET~~

~~SECRET - SECURITY INFORMATION~~ 15 July 1953

1. The Department of Defense agrees 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 the 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 proper sense of the NSC and general clarity should be reworded. 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 following word changes be made:

a. In paragraph 1 e (2) - page 3 line 16, ~~line 10~~, delete "shall make such recommendations" and insert "will take such action".

Reason - The Board must be strong and have the authority to take action to ensure compliance with its decisions. If the Board is not given this clear and indisputable authority to direct compliance, all disagreements will have to go to the President for resolution. This obviously is impractical and not intended by the President as expressed by his memorandum of 24 October 1952.

b. In paragraph 2 b, ~~line 4~~ - after the phrase "departments and agencies of the government" add "and to adjudicate disputes arising from decisions of the Director, NSA".

Reason - The departments and agencies must have some procedure for appealing a technical decision of the Director, NSA. It is not realistic to expect the non-technical Board to settle wisely a disagreement about a technical decision. This addition gives the departments additional protection by providing a way for such disputes to be settled on their technical merits.

c. In paragraphs 2 c (1) (a) and (b) - delete the opening phrase "Subject to review by the Board in the event of disagreement". Page 8 lines 9 + 16

Reason - The Board is not a technical group and hence is not equipped to deal competently with technical questions. There is a valid need for an outlet for technical disagreements. However, [redacted] the change given above for paragraph 2 b provides such a procedure and keeps it in the technical area. Any disagreements which start as technical ones but which cannot be settled by the Secretary of Defense and persist and grow into policy disputes can then be handled by the appeal procedure given in paragraph 1 g and h.

d. Also in paragraphs 2 c (1) (a) and (b), Page 8 line 16 ~~line 2~~ - replace the words "review and approve" with the word "prescribe".

Reason - The adequacy of U. S. cryptosystems can be ensured as required by the President's memorandum of 24 October 1952 only by centralizing the responsibility and authority to determine the fundamental principles used in the specific cryptosystems and the operating procedures needed to realize the full potential of the principle. This determination, which includes reviewing and evaluating existing principles and procedures and devising and evaluating new ones, is based on cryptanalysis and utilizes lessons learned from study of foreign traffic. Thus, it cannot be separated from the nations COMINT activity. Absolute control is essential to prevent the use of a weak cryptoprinciple by one department which could be solved by the enemy and pave the way for solving stronger cryptoprinciples. Similarly, weak procedures and poor cryptosecurity standards can undermine the strongest cryptoprinciples and lead to solution. Thus, the establishment of an appropriate authority to assure high and uniform standards of COMSEC as directed by the President can be done only by designating one authority ~~NSA~~ as prescribing ~~authority for~~ for cryptoprinciples and procedures. This KCC heaps COMSEC and COMINT closely bound together and guarantees a better product from each.

e. In paragraph 2 c (1) (d) - Insert at the beginning of the paragraph the phrase "Under policies promulgated by the Board and"

page 9 lines 6 to 12

e. In 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 - Technical liaison with cooperating foreign agencies on COMSEC matters has a direct effect on the conduct of COMINT activities, close liaison on sharing production workload. Careful control over the disclosure of U. S. cryptoprinciples to foreign nations is absolutely essential to avoid inadvertently setting the COMINT effort back several years or worse eliminating a fruitful source of intelligence. Further close working level liaison is essential to obtain maximum economy in the provision to and exchange of COMSEC materials needed to protect US - UK and NATO communications. Note that it is not proposed to have the Director, NSA conduct liaison at diplomatic level nor to conduct all COMSEC liaison but for protection of COMINT he must have cognizance over the conduct of all of it. The proposal of policy determination by the USCSB and cognizance over implementation

by the Director, NSA assures that effective coordination of COMSEC problems with respect to foreign governments as desired by the President is achieved with technical soundness.

f. In paragraph 2 c (1) (g): Page 10

In line 2, delete phrase "Subject to approval by [redacted]".

Reason - Approval authority over long range plans for COMSEC is given to the Board in paragraph 1 e (3)(b)(4). Restating this authority here adds nothing to the Directive.

In line 5, delete phrase "consisting of projects of common concern which can be more efficiently accomplished centrally" and in 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 orderly, early and effective exploitation, authority and responsibility for COMSEC research and development should be centralized. The organization responsible for prescribing cryptoprinciples and cryptosecurity procedures should, therefore be assigned cognizance over the national COMSEC research and development program. This organization should be empowered to make the most technically feasible, economical, and effective use of the limited amount of communications security development talent available to the United States. It should be responsible for the formulation of an overall COMSEC research and development program, for the conduct of a major portion of the

program, and for effective utilization of the research and development facilities of the various departments and agencies of the government. It should not be restricted to "projects of common concern" as has been proposed if the overall COMSEC program is to be effective in assuring a satisfactory state of cryptosecurity. From the technical viewpoint, it is essential to national security that the U. S. COMSEC agency maintain continuously an integrated research and development program, rather than merely "review and coordinate" a diversity of COMSEC development programs. This authority, in order to be effective in achieving the objectives set forth in the Presidential Memorandum of 24 October 1952, should include the functions and responsibilities described by the suggested revision of subpara. g. The statement as revised, (1) Establish the authority necessary to insure both economy and high, uniform protection for classified Federal telecommunications, and (2) Provide the most effective means of promoting initiative in all the departments and agencies interested in COMSEC research and development.

g. In paragraph 2 c (1)(h):

In line 2, delete the phrase "insofar as practicable" and in line 3 after the words, "the comptability" add the words, "and insofar as practicable standardization".

Reason - The compatability of crypto-equipments is essential to inter-communication while different conditions call for

different shapes and construction, crypto-equipments designed for the same general communication purpose must be cryptographically compatible, i.e. able to work together. Standardization of techniques, parts, and materials to the greatest extent possible consistent with the intended application of the equipment, will held reduce the cost of and will simplify manufacturing maintaining, and using the equipments.

h. In paragraph 2 c (1)(i): page 11 lines 1 to 4

In line 3, 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.

i. In paragraph 2c(1)(j) page 11

Add new paragraph j to read, "Nothing in this directive shall be construed as precluding the Director, NSA of 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 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 operation must be kept in operation.