STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO C/S

DATE 14 Jul 53

FROM : C/SEC

SUBJECT Proposed NSC Directive for COMSEC

1. Attchd is recommended comment to the 3 July draft of NSC Directive and a proposed revision of same with a view to firming up the Department of Defense position prior to the forthcoming meeting. Colonel Many has seen this; R&D apprsd in preparation, and P/P furnished copy this draft. JSC

~~SECRET - SECURITY INFORMATION~~

13 July 1953

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

SUBJECT: Proposed NSC Directive for COMSEC

1. The Presidential Memorandum of 24 October 1952, subject: "Communications Security" directs action to establish effective, efficient, and economical means for assuring the security of classified Federal telecommunications. The Department of Defense takes the position that this can only be done by (1) designating a technically competent operating organization to act for the entire Government, and (2) a policy making board empowered to insure compliance. It considers that the draft NSC Directive of 3 July 1953 on COMSEC accomplishes only the latter.

2. The security of Federal telecommunications is of paramount importance. It would be contrary to the spirit of the Presidential memorandum to attempt to assure this security by relying upon voluntary coordination and cooperation among the departments or upon an unwieldy board. Centralized responsibility for the complete technical operation involved is absolutely necessary and is not provided in the proposed NSC directive. Specifically, the draft version fails in the following respects:

a. Does not assign complete and clear responsibility for the adequacy of cryptoprinciples.

b. Does not assign complete and clear responsibility for the determination and adequacy of general cryptosecurity rules and procedures for operating cryptosystems.

c. Does not provide an effective and economical means for marshalling the research and development effort necessary to ensure the continuing adequacy of U. S. COMSEC.

d. Does not provide adequately for the conduct and coordination of technical liaison with foreign governments and international organizations on COMSEC matters.

e. Does not provide for a responsible authority to standardize, produce, and procure COMSEC materials and equipments.

3. The Department of Defense considers it essential to the implementation of the Presidential memorandum that the NSC directive assign the specific functions and responsibilities in these areas to the Director, NSA and the authority to insure compliance to the U. S. COMSEC Board. It is considered that the National Security Agency is

the only appropriate authority to assure that the U. S. has high and uniform standards of COMSEC and adequate cryptographic systems and that to do this requires the centralization of responsibility in the National Security Agency for prescribing cryptoprinciples, minimum cryptosecurity standards, and procedures for operating cryptosystems, for having cognizance over and conducting technical liaison with the cryptologic agencies of foreign nations and international organizations, and for programming and conducting or supervising the national COMSEC research and development effort. This carries out the President's view of communications security as a national responsibility. It promotes economy by opening practical and effective ways for standardization of materials and the coordination and resolution of interdepartmental problems.

4. The position stated above derives directly from the experience of the Director, NSA over a period of years in dealing with the complete range of technical activities involved in COMSEC on a scale which is so broad and constitutes such a major portion of the total U. S. COMSEC effort as to be almost national in scope. This has included the development of the fundamental principles employed in the major crypto-equipments used by the Government; the evaluation and continuous re-evaluation of the strength of these principles and the specific methods by which they are applied and used; almost daily contact on technical problems with the representatives of the cryptologic organizations of cooperating foreign nations and NATO; the programming and conduct of basic research on physical and mathematical phenomena which appear to be applicable to COMSEC purposes, and the development and engineering of COMSEC equipment.

5. It is essential that the responsibilities of the Director, NSA acting for the Executive Agent be changed substantially as shown in Appendix "A" for the reasons given briefly above and explained more fully in Appendix "B".

2 Incls:
1. Appendix A (Revision of Portion of Proposed NSC Directive on COMSEC Covering Responsibilities of Executive Agent)
2. Appendix B (Considerations Supporting the Position of the Director, NSA)

~~SECRET~~ ~~SECURITY INFORMATION~~

APPENDIX A

Revision of Portion of Proposed NSC Directive on COMSEC Covering Responsibilities of Executive Agent

1 The revision of paragraph 2 c (1) given below is considered essential to cover and clearly assign the functions and responsibilities necessary to implement the provisions of the President's Memorandum of 24 October 1952 The wording has been altered in sub-paragraphs a, b, d, e, f, g, and h, sub-paragraph c is kept unchanged, and sub-paragraph i is deleted as being premature and inappropriate for a general basic directive Also wherever appearing, the phrase "Subject to review by the Board in the event of disagreement " has been deleted as a redundancy in view of the general, overall, review authority which properly is designated in the Board in paragraph 1 e and the appeal procedure set up in paragraph 1 g.

2. The detailed revision follows.

Paragraph 2 c (1):

(a) Devise and prescribe the basic cryptoprinciples embodied or to be embodied in telecommunications equipment, COMSEC equipment, or cryptosystem, giving full consideration to recommendations received from the departments or agencies

(b) Devise and prescribe procedures necessary to operate in a secure manner the specific embodiments of cryptoprinciples, and devise and prescribe general rules and minimum cryptosecurity standards applicable to operations common to all cryptosystems,

review and approve procedures devised to meet requirements unique to any department or agency.

(c) Perform technical analysis of Federal telecommunications for purposes of determining the degree of cryptosecurity being provided by the crypto-principles, materials, and procedures utilized by the departments and agencies, as well as the effect thereon of communication procedures and practices; and make necessary arrangements, as appropriate, to obtain the material required for such analysis; (see paragraph 3-b)

(d) Under policies promulgated by the Board, and subject to the exception granted the Director of the Central Intelligence Agency under NSCID No 5, conduct or coordinate the conduct of liaison on the technical COMSEC and related matters with the cryptologic agencies of foreign nations and international organizations.

(e) In consonance with policies of the Board, provide technical guidance and support for cryptosecurity training conducted by the departments and agencies.

(f) Obtain from the departments and agencies their requirements for COMSEC equipments and materials; formulate, for consideration by the Board, integrated programs for the

~~SECRET - SECURITY INFORMATION~~

production, procurement, and maintenance thereof;* and implement the approved program by internal action, commercial contract, and delegating to the departments and agencies those portions which they desire and which can be performed most effectively by them.

(g) Formulate for approval of the Board and maintain continuous review of an integrated COMSEC research and development program which is sufficient to assure the continuing security of Federal telecommunications. Establish and conduct (internally and by contract) COMSEC research and development projects necessary to implement the approved program. The departments and agencies are authorized to pursue research and development projects designed to meet their special needs providing the Director, NSA reviews and approves such projects prior to their initiation.

(h) In meeting operational requirements, the Director of the National Security Agency will insure, insofar as those requirements will permit, the standardization of COMSEC materials and equipments in order to promote efficiency and economy in their procurement, operation, and maintenance. Determination of the acceptability of the physical embodiments of cryptoprinciples is a function of the various departments and agencies.

* Insofar as the Department of Defense is concerned, these programs will include budgeting details which specify, among other items, the funding required by the military departments and agencies.

~~SECRET - SECURITY INFORMATION~~

APPENDIX B

CONSIDERATIONS SUPPORTING THE POSITION OF THE DIRECTOR, NSA

1. Responsibility for prescribing cryptoprinciples.

a. The responsibility for prescribing, reviewing, and approving cryptoprinciples is the heart of the President's desire to insure that the U. S. has adequate cryptographic systems and high and uniform standards of communications security. A cryptoprinciple suitable for use today must be so rigorously analyzed mathematically that it requires a technically competent organization. In the interests of getting the maximum concentration of technical ability within a price the nation can afford, it must be done in one organization and not in several. It would not matter which organization in the government did this work if it were not for this important fact, viz; COMINT and COMSEC are inextricably related and the effective conduct of each varies directly with the completeness and intimacy with which the operations of both are coordinated. The Brownell Committee in its report on U. S. COMINT operations took special note of this relationship and emphasized the absolute necessity for keeping the COMSEC and COMINT activities closely tied together.[1] This interrelationship makes it possible for the government to utilize in the most effective manner the very limited number of competent cryptanalysts available to the U. S. in the analysis of our own cryptosystems, to take direct, immediate, and demonstrably effective corrective action when a weakness in one of our systems is revealed in cryptanalyzed traffic of a foreign nation, or

1. Page 101, Brownell Committee Report

to take preventive action based upon the method by which a cryptanalytic breakthrough has been achieved.

b. There is a trend today away from separate and distinct crypto-equipments and towards the integration of cryptosecurity elements in telecommunication equipment. In every respect this is desirable; however, it promises to present policy and administrative complications, for there are many distinct organizations within the government having responsibility for the development of telecommunication equipment. It would be uneconomical, inefficient, and ineffective to require them to assemble competent cryptologic staffs to devise, analyze, and perfect cryptoprinciples for use in telecommunications equipment. The continued existence of a central source to which they can look for a crypto-principle will keep them free to concentrate on the communications portion of the development, will provide a common point for the exchange and coordination of ideas on the integration of security principles into telecommunication equipment, and will assure effective control of the release of cryptoprinciples to usage in equipments destined to have widespread (even commercial) applications in the telecommunication field. A national COMSEC organization would serve all COMSEC consumers as the source of basic instruction essential for clarification of procedures and establishment of new procedures to meet new situations.

c. If the responsibility to prescribe cryptoprinciples is not centralized, each department or agency would be permitted and expected to establish its own criteria and prescribe the cryptoprinciples which it desired to use. The demonstrated quality of the principles

could be only as good as the mathematical analysis and cryptanalytic effort applied to it. The consequences would be that among those agencies which realize this there would be a scramble for the limited amount of talent trained and capable of performing this analysis, and as usual the agencies with the most money, though not necessarily the greatest need, would obtain them and have a relatively high security in their systems. The others would have well-intentioned but amateurish efforts at security. Under such conditions, the nation would suffer for there would be no effective means of achieving high and uniform standards of security nor of insuring the adequacy of the cryptographic systems used.

d. It is contended that dispersion of this responsibility would be a fatal weakness, that cooperation among the several departments cannot be substituted for a central authority, and that a reviewing function would be insufficient to satisfy the objectives of the President's directive of 24 October 1952. Witness the experience of the last few years in the COMINT field as set forth in the Brownell Committee report.[2] The Brownell Committee found that the authority and responsibility established by the Secretary of Defense directive of 1949 (the AFSA Charter) which represented an advance toward centralized functions and responsibilities, did not centralize sufficiently to provide the opportunity for maximum or even adequate effectiveness in military COMINT-COMSEC operations. An historical example of hazard to national security resulting from failure to

2. Page 121 Brownell Committee Report

centralize COMSEC technical responsibilities was provided by Germany during World War II. The story of the German cryptosecurity failures is well documented[3] and it can be stated unequivocably that the German experts attributed this failure largely to the fact that the responsibilities and the scientific talent for planning, guiding, and conducting German cryptologic activities were spread thinly over 6 to 8 separate agencies.

e. Thus, it is imperative that the responsibility of prescribing, reviewing, and approving cryptoprinciples be centralized and be kept with the responsibility for conducting U. S. COMINT operations; specifically, the Director, NSA.

2. Prescription of Crypto-operating Procedures.

a. After determination of the cryptoprinciple to be employed and development of equipments and systems embodying such crypto-principles, there remains the prescription of general minimum standards for all cryptographic operations, and the devising of instructions and procedures specifically applicable to the operation of a particular crypto-equipment or system. General cryptosecurity rules and regulations are those which are concerned with those aspects of crypto-operations common to all crypto-equipment and systems. They are the minimum standards which guide the conduct of those aspects and must be uniform to avoid jeopardizing national security interests. To insure that insecurities do not exist in one agency which would jeopardize the security of another, it is essential that minimum standards common to all agencies and departments be prescribed by the authority having

3. e. g., DF 249

primary cognizance of national communications security. Supplemental or explanatory rules may be necessitated by requirements peculiar to a particular agency.

b. Instructions and procedures necessary for the operation and use of a particular crypto-equipment or system always affect the degree of protection afforded by that equipment or system. To insure attainment of maximum security the most effective and secure method and procedure for operation must be used. It is therefore essential that the responsibility for prescription of operating rules and procedures rest with the authority responsible for the development of cryptoprinciples, since that authority alone would be in a position to discharge it. It is recognized that ideas are not exclusive to any one individual or group. Therefore, it is the more important that procedures and rules to improve operations and security should be devised anywhere, and that there should be a means for these to become available to all. The establishment of a single authority to review, evaluate, and promulgate ideas applicable to the operation of crypto-systems is the only economical, efficient, or effective method of realizing this objective.

c. Moreover, it is essential that the responsible COMSEC authority have immediate and continuing access to the national COMINT effort, since determination of the most effective and secure method of operation is continually influenced by knowledge of the mistakes and accomplishments of other nations. Advantage of such information can be taken most expeditiously if the authority to prescribe operating

procedures is centered in the organization which is also responsible for the production of COMINT.

3. Research and Development.

a. The authority responsible for the prescription of crypto-principles and of cryptosecurity operating procedures must have cognizance over the national communications security research and development program. This authority must 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 must be responsible for the formulation of an overall COMSEC research and development program, for the conduct of the major portion of such a program, and for the most effective utilization of the research and development facilities of the various departments and agencies of the government. It cannot be limited to "projects of common concern" as has been proposed, with any hope of achieving an economical, integrated program. To the extent that communications security is of national concern, the cryptoprinciples and crypto-equipments developed anywhere in the world for the potential use of any organization of the government are matters of a national interest, inasmuch as a weak system used by one department or agency is thoroughly capable of nullifying the protection afforded by a sound system employed by all the other departments and agencies of the government. Therefore, seen from the technical viewpoint, it is essential to the national security that the U. S. COMSEC authority supervise an integrated research and development program rather than

~~SECRET - SECURITY INFORMATION~~

merely "review and coordinate" a diversity of COMSEC development programs.

b. This supervision, in order to be effective in achieving the objective set forth in the Presidential Memorandum of 24 October 1952, must include authority and responsibility for establishing the overall program, for conducting the major portion thereof, for reviewing the program frequently, and for assigning and supervising those elements of the program which can be most effectively conducted by the various departments and agencies. This is considered to constitute the minimum authority necessary to provide any significant assurance of high and uniform protection for classified Federal telecommunications.

c. For effective operation, the conditions under which COMSEC research and development projects will be initiated and carried out by the various departments and agencies should be clearly specified. Also, the COMSEC authority should be charged with mobilizing all appropriate research and development facilities of the government in the most effective manner possible. This can be done and should be set down in a manner which will <u>not</u> stifle, nor even suggest the stifling of, initiative in any agency or department; rather it should positively encourage the submission of ideas for orderly, expeditious, and effective exploitation in the interest of national security.

4. <u>Foreign Technical Liaison</u>.

a. Because of the effect that the conduct of foreign liaison in the cryptographic field might have on the discharge of his assigned responsibilities for the national COMINT effort, it is considered

necessary that the Director, NSA have primary cognizance over the conduct of liaison. The conduct of the national COMSEC effort without authority to conduct technical liaison on COMSEC matters with foreign and international activities having similar responsibilities would be neither efficient, economical nor effective.

b. It is not proposed that all COMSEC liaison be conducted by the Director, NSA. Neither is it intended that liaison be conducted by the Director, NSA at the diplomatic level. However, it is proposed that he continue to be responsible for the conduct of the type of technical liaison with cryptologic activities of the allied and NATO nations which is presently being conducted on an almost daily basis. This daily liaison is exemplified by authorized exchanges of evaluations of the security of cryptoprinciples with the communications security organization of the U. K., to insure that the security standards of closely allied nations are sufficiently high to protect information vital to the security of this nation. Similar exchanges in research engineering and development matters have provided a means of insuring that new developments and techniques of other nations may be quickly and effectively utilized by the United States.

c. Therefore, it is proper that the cognizance over such liaison be clearly assigned to the Director, NSA. The national policies under which this liaison is carried out should be established and promulgated by the U. S. COMSEC Board, but in the interest of effective operations the conduct of such liaison should not be subjected to detailed direction by the Board.

~~SECRET - SECURITY INFORMATION~~

5. The Brownell Committee in its conclusions and recommendations to the President[4] stated that the conduct of communications security is a portion of the total cryptologic program of the nation, and as such must be integrated with the conduct of the COMINT activities. Granting that COMSEC is a portion of the cryptologic effort of the country, its relation to COMINT activities is closest in the prescription of the cryptoprinciples, the engineering by which these principles are embodied and the procedures by which they are applied in actual usage. Therefore, it is clear that the Brownell Committee, which recommended a strengthening of the increased centralization of this effort and the assignment of definite responsibility to and effective authority of the Director intended that the total cryptologic effort be so placed and so directed.

4. Page 9, Brownell Committee Report