

REF ID:A72215

EXECUTIVE OFFICE OF THE PRESIDENT  
NATIONAL SECURITY COUNCIL  
WASHINGTON

~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

July 7, 1953

MEMORANDUM FOR: Mr. Robert R. Bowie  
Mr. Elbert P. Tuttle  
Mr. Thomas J. Donegan  
Mr. Frank C. Nash  
Major General John K. Gerhart  
Mr. Robert Amory, Jr.  
Mr. Roy B. Snapp

SUBJECT: Communications Security

The enclosed Draft NSC Directive on the subject, prepared by an ad hoc group consisting of representatives of the Departments of State and Defense, the Federal Bureau of Investigation and the Central Intelligence Agency, is transmitted herewith for consideration at an early meeting.

S. EVERETT GLEASON  
Acting Executive Secretary

~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~D R A F T

FOR NSC STAFF CONSIDERATION ONLY  
(Planning Board)

July 3, 1953

NATIONAL SECURITY COUNCIL DIRECTIVE

on

COMMUNICATIONS SECURITY

The Presidential directive of October 24, 1952:

a. Stated that the security of Federal telecommunications (COMSEC) is a national responsibility, and that COMSEC policies and procedures must be integrated so as to enable the various departments and agencies of the Government to cooperate effectively in such matters and to satisfy legitimate requirements for the security of their messages;

b. Designated the Secretaries of State and Defense as a Special Committee of the National Security Council for COMSEC matters, to establish such policies relating to COMSEC as will achieve the maximum security of Federal telecommunications, and to keep the President advised of such policies through the Executive Secretary of the National Security Council\*; and

\*The President in approving this directive also directed that the Attorney General shall be a member of the Special Committee whenever matters of interest to the Federal Bureau of Investigation are before that committee. In accordance with the President's instructions regarding the normal operation of the Council, the heads of departments and agencies not represented on the Special Committee, shall also participate as members of the Special Committee whenever matters of direct interest to their respective agencies are before that Committee.

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

D R A F T

c. Directed the Special Committee of the NSC to prepare and issue in the COMSEC field directives which will:

(1) Rescind the Executive Order of July 3, 1945 entitled "Cryptographic Security with Respect to Certain Communications of the Government".\*

(2) Establish a United States Communications Security Board (USCSB) responsible for integrating policies and procedures affecting the security of Federal telecommunications.

(3) Provide for the establishment of appropriate responsibilities and authorities to assure within the various departments and agencies of the Government, among other things:

(a) High and uniform standards of communications security;

(b) Effective cooperation in COMSEC matters between departments and agencies concerned;

(c) The adequacy of the cryptographic systems used;

(d) Coordination of COMSEC problems, particularly policies with respect to foreign governments;

(e) Satisfaction of legitimate requirements for the security of telecommunications.

\*The Order was classified and was not published in the Federal Register. It was rescinded by the President on           (date)          .

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

Pursuant to the foregoing and to the provisions of Section 101 and Section 211 of the National Security Act of 1947, as amended, the Special Committee of the National Security Council for COMSEC hereby authorizes and directs as follows:

1. The United States Communications Security Board (USCSB):

a. There is hereby established the United States Communications Security Board (USCSB), hereinafter referred to as the Board, which shall be a body acting for and under the aforesaid Special Committee and shall operate in accordance with the provisions of this Directive and any other directives which may be issued by the Special Committee.

b. The Board shall be composed of one representative of each of the following:

- (1) The Secretary of State
- (2) The Secretary of Defense
- (3) The Secretary of the Treasury
- (4) The Director, Federal Bureau of Investigation
- (5) The Secretary of the Army
- (6) The Secretary of the Navy
- (7) The Secretary of the Air Force
- (8) The Director of Central Intelligence
- (9) The Director of the National Security Agency
- (10) The Atomic Energy Commission

c. The Board shall elect its own Chairman from among its membership.

D R A F T~~CONFIDENTIAL  
SECURITY INFORMATION~~

d. The Board shall have a staff headed by an executive secretary who shall be appointed by the Chairman with the approval of a majority of the Board.

e. The Board shall have the following responsibilities:

(1) To integrate policies and procedures affecting the security of Federal telecommunications;

(2) To establish, under authority of the Special Committee, such communications security policies as will insure high and uniform standards of communications security within the various departments and agencies of the Government and will achieve the maximum practicable degree of security of Federal telecommunications. For this purpose, the Board shall study the standards and practices of any department or agency in the field of communications security; and the Board shall make such recommendations as may be necessary to assure compliance with its decisions in this field;

(3) To establish broad policies necessary to:

(a) Institute and maintain effective cooperation in communications security matters among the departments and agencies concerned, and

(b) Satisfy legitimate requirements for the security of the communications of the departments and agencies;

D R A F T~~CONFIDENTIAL  
SECURITY INFORMATION~~

(4) To approve the long-range plans for the communications security of the United States;

(5) To establish policies affecting relations of the U. S. Government with foreign governments and international organizations in communications security matters;

(6) To advise the Special Committee with respect to communications security policy matters decided by the Board and make recommendations as appropriate; and

(7) To establish policies and appropriate procedures governing actions to be taken by the Executive Agent in COMSEC matters.

f. The Board shall meet at the call of the Chairman or at the request of any member, and shall determine its own procedures subject to the provisions of this Directive.

g. The Board shall reach its decisions by majority vote. In the event that the Board votes and reaches a decision, any dissenting member of the Board may appeal from such decision. Such appeal must be made within 15 days to the Special Committee. In the event that the Board votes and fails to reach a decision, any member of the Board may appeal to the Special Committee and such

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

appeal must be made within 15 days of the inconclusive vote. In either event the Special Committee shall review the matter, and its determination thereon shall be final. Appeals by the Director of NSA, or by the representative of any of the Military Departments shall be filed only with the approval of the Secretary of Defense.

h. No action shall be taken with respect to any matter forming the subject of an appeal until the appeal is decided; provided that, if the Secretary of Defense determines, after consultation with the Secretary of State (and the Attorney General and the heads of other departments and agencies as appropriate), that the subject matter presents a problem of an emergency nature and requires immediate action, his decision shall govern, pending the result of the appeal. In such an emergency situation the appeal may be taken directly to the President by the Special Committee.

i. The Board shall invite the head of any department or agency not represented on the Board to designate a representative to participate with the Board in consideration of matters of direct interest to such a department or agency, to the end that the communications security needs of all such departments and agencies may be considered; and heads of departments or agencies not

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

represented on the Board may present, through the Executive Secretary of the Board, communications security matters for consideration by the Board.

1. Departments or agencies not represented on the Board may appeal from decisions of the Board in the manner prescribed for departments and agencies represented on the Board.

2. The Department of Defense:

a. The Department of Defense is hereby designated as Executive Agency of the Government.

b. As Executive Agency, the Department of Defense is charged with mission of:

(1) Providing for the Board, centralized, overall cognizance and authoritative supervision of the measures necessary to provide and assure the adequacy of the COMSEC techniques and materials used by the government;

(2) Formulating for the Board integrated technical and operating policies, programs, and long range plans required to maintain high and uniform standards to ensure the security of Federal <sup>telecommunications,</sup> and

(3) Providing advice and recommendations on any aspect in the field of communications security.

the Special Committee for immediate decision.

d. Subject to the specific provisions of this Directive and subsequent directives as may be issued, the



D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

Director of the National Security Agency (NSA) shall act for the Executive agent in the COMSEC matters which are set forth in subparagraphs (1) through (4) below and which may be specified by the Special Committee or the Board. With respect to the Military Departments, the Director of NSA will perform his functions under the immediate direction of the Joint Chiefs of Staff.

(1) Cryptosecurity

(a) Prescribe or review and approve

the

crypto-principles incorporated or to be incorporated in any telecommunications equipments and systems and in any communications security equipments and systems used by the departments and agencies of the Government.

(b) Prescribe or review and approve

crypto-

security rules, regulations and instructions applicable to the operation and use of any crypto-equipments and systems and of any communications security equipments and systems,

(c) Perform technical analysis of Federal telecommunications for purposes of determining the degree of cryptosecurity being provided by the crypto-principles, materials, and procedures

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

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) Conduct liaison on technical COMSEC and related matters with the cryptologic authorities of foreign nations and international organizations.

(e) Provide technical guidance and support for cryptosecurity training conducted by the departments and agencies.

(f) Obtain from the departments and agencies their requirements for crypto-equipments and materials, and formulate for consideration by the Board integrated programs for the production and procurement thereof;\*

\*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.

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

(g) Provide for review and coordination of cryptosecurity research and development programs; and establish and conduct an adequate research and development program. Departments and agencies are not precluded from initiating and, subject to prior notification to and approval by the Director of NSA from pursuing such research and development as may be necessary to support their cryptosecurity activities;\*

(h) In meeting operational requirements the Director of NSA will insure the compatibility and, insofar as practicable, the standardization of crypto-equipments and material in order to promote maximum efficiency and economy in their procurement, operation and maintenance. Determination of the acceptability of the physical embodiments of crypto-principles 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.

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

(i) The Director of NSA will furnish services and materials for the COMSEC programs of the departments and agencies on a fiscal arrangement as mutually agreed with the departments and agencies.

(j) 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 <sup>from</sup> producing, printing, procuring, and modifying cryptomaterials to meet the requirements of the departments and agencies or from budgeting for the conduct of his activities.

necessary technical analysis of Federal telecommunications, making arrangements, as appropriate, with departments and agencies to obtain the material required for such analysis. (See paragraph 3-c).

(3) Physical security:

The Director of NSA will, in collaboration with the departments and agencies, as appropriate, prescribe minimum standards for physical security of cryptosystems and related cryptomaterial.

\*Applicable only to departments and agencies outside the Department of Defense.

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~(4) Cover and Deception:

The Director of NSA will, in collaboration with appropriate departments or agencies, assist in the preparation of, and review the communications portions of all strategic cover and deception plans, and formulate and promulgate the basic policies utilized in such portions.

e.g. The Director of NSA shall exercise his authority over communications security matters under his cognizance through the agency representatives on the Board or, in the case of agencies not represented on the Board, through the duly authorized representatives of the heads of such agencies. <sup>Arrange</sup> Where ~~liaison~~ with subordinate elements of a department or agency is considered necessary, the Director of NSA shall arrange with the authorized representatives of the departments or agencies concerned for such liaison.

f.g. The Director of NSA is authorized to obtain from the departments and agencies such information as he may require in performing his functions, as authorized in this directive or any other directive subsequently issued.

g.g. The Director of NSA shall have neither the responsibility nor the authority to compel, within organizations other than his own, compliance with communications security instructions issued by any authority, but shall

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

refer violations of such instructions outside his Agency to the chief or head of the organization concerned for such action as may be deemed necessary. If appropriate corrective action is not taken and violations continue, the Director, NSA, shall refer the subject to the Board.

3. Departments and Agencies of the Government:

a. All decisions of the Board, or of the Special Committee, which are not in conflict with law shall be binding on all departments and agencies of the Federal Government.

b. No department or agency of the Government shall be required to disclose to the Director of NSA, or to the Board, or to any of its committees, the contents of any official communication concerning its activities if, in the opinion of the head of such department or agency, the disclosure would be contrary to the National interest, and nothing in this Directive shall be construed to give the Board or any of its representatives the right of inspection of any department or agency without approval by the head thereof.

c. Subject to the provisions of law, the directives of the President, the provisions of this Directive, and any other directives which may be issued by the Special Committee, the departments and agencies of the Government

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

will organize and conduct their communications security activities as they see fit, and nothing in this Directive shall relieve the individual departments and agencies of their responsibilities for executing all measures required to assure the security and efficiency of their own telecommunications.

d. All rules and regulations in conflict with the provisions of this Directive shall be brought to the attention of the Board.

4. Special Terms Used in this Directive are Defined as Follows:

a. Telecommunications - Any transmission, emission or reception of sign, signals, writing, images and sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic system.

b. Federal Telecommunications - Those telecommunications which are of an official character dealing with governmental affairs and are originated by or intended for officials of the United States Government. Specifically exempted from this definition is that portion of the communication activities conducted by the Central Intelligence Agency in accordance with the authorities granted the Director of Central Intelligence under NSCID No. 5.

D R A F T~~CONFIDENTIAL~~  
~~SECURITY INFORMATION~~

c. Communications Security - The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study. Communications security includes: (1) transmission security; (2) cryptosecurity, and (3) physical security of communications security materials and information.

d. Transmission Security - Transmission security is that component of communications security which results from all measures designed to protect transmissions from unauthorized interception, traffic analysis, and imitative deception.

e. Cryptosecurity - That component of communications security which results from the provision of technically sound cryptosystems and their proper use.

f. Cryptoprinciple - The characteristics of the elements involved in, and the fundamental rule of operation, motion, or activity inherent in a cryptosystem.

g. Cryptosystem (Cryptographic System) - The associated items of cryptomaterial which are used as a unit and which provide a single means of encryption and decryption.



D R A F T~~CONFIDENTIAL  
SECURITY INFORMATION~~

h. Cryptomaterial - All material, including documents, devices and/or equipment or apparatus employed in the encryption or decryption of telecommunications.

i. Crypto-equipment - The crypto-apparatus, mechanisms, machines or devices used in the encryption or decryption of telecommunications.

i. Physical Security - That component of security which results from all physical measures necessary to safeguard classified equipment, material and documents from access thereto or observation thereof by unauthorized persons.