

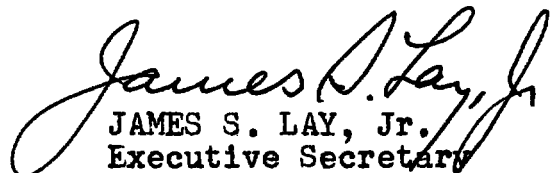
EXECUTIVE OFFICE OF THE PRESIDENT
NATIONAL SECURITY COUNCIL
WASHINGTON

June 23, 1953

MEMORANDUM FOR: Mr. S. D. Ellis
Mr. William F. Friedman ✓
Major General H. M. McClelland, USAF (Ret.)
Mr. Lee W. Parke
Colonel George P. Sampson
Mr. William D. Wright

SUBJECT: Proposed NSC Directive on COMSEC

Enclosed is the draft proposed NSC directive on COMSEC as revised at the meetings on June 16 and 19, 1953. The enclosure is scheduled for further consideration at a meeting on Friday, July 3 at 10:00 a.m.


JAMES S. LAY, Jr.
Executive Secretary

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

June 19, 1953

NATIONAL SECURITY COUNCILCOMMUNICATIONS SECURITY DIRECTIVE NO.

Pursuant to the ^{provisions and to the} provisions of Section 101, ^{and Section 211} of the National Security Act of 1947, as amended, and to ^{the} Presidential directive of October 24, 1952; ~~which~~

move down

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 on 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 Secretary of the Treasury and the Chairman, Atomic Energy Commission, shall also participate as members of the Special Committee whenever matters of direct interest to their respective agencies are before that Committee.~~

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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 3 July 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) .

~~CONFIDENTIAL~~

Pursuant to the foregoing etc~~CONFIDENTIAL
SECURITY INFORMATION~~

the Special Committee of the National Security Council for COMSEC hereby authorizes and directs that:

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.

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;

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

(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 may 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;

(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; ...

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

(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 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

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

is decided; provided that, if the Secretary of Defense determines, after consultation with the Secretary of State, (and the Attorney General 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.

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

i. 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. ^{Department} The Secretary of Defense:

a. ^{Department} The Secretary of Defense is hereby designated as Executive Agent of the United States Communications Security Board for all COMSEC matters.

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

Dept
b. As Executive Agent the Secretary of Defense is empowered to take action within policies and procedures established by the Board, in all COMSEC matters affecting the departments and agencies of the Government provided, however, that where exception to his action is made by the Secretary of a department or by the Head or Director of an agency outside of the Department of Defense, such exceptions shall be referred to the Board. Pending Board review, if the Secretary of Defense determines that the subject matter presents a problem of an emergency nature and requires immediate action he may refer the matter to the Special Committee for immediate decision.

c. Subject to the specific provisions of this Directive and subsequent directives as may be issued, the Director of the National Security Agency (NSA) shall act for the Executive agent in COMSEC matters as set forth below and as 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) Subject to review by the Board in the event of disagreement, review and approve

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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

in any communications - security equipments and

(b) Subject to review by the Board in the event of disagreement review and approve cryptosecurity rules, regulations and instructions applicable to the operation and use of any crypto-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 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) Subject to the authority granted the Director of Central Intelligence under NSCID No. 5, coordinate and review for the Board the conduct of foreign liaison in such matters by departments and agencies of the Government and conduct such liaison as directed by the Board;

cryptosecurity and related

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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

(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;

(g) In consonance with the policies of, and subject to approval by, the Board, provide for review and coordination of cryptosecurity research and development programs; and establish and conduct a research and development program consisting of projects of common concern which can be more efficiently accomplished centrally. Departments and agencies are not precluded from initiating and, subject to prior notification to and coordination with the Director of NSA, from pursuing such research and development as may be necessary to support their cryptosecurity activities.

;

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

(h) In meeting operational requirements the Director of NSA will insure, insofar as practicable the compatibility of crypto-equipments and material in order to promote maximum efficiency and economy in their *production,* procurement, ~~operation~~ and maintenance. Determination of the acceptability of the physical embodiments of crypto-principles is a function of the various departments and agencies;

(i) The Director of NSA will furnish services and materials for the COMSEC programs of the departments and agencies only on a reimbursable basis.

(2) Transmission security:

The Director of NSA shall be responsible for review and evaluation of communications procedures developed by the departments and agencies, to determine if such procedures will insure the maintenance of transmission security, recommending revisions and additional rules and procedures as required. To accomplish this the Director of NSA may perform 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).

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

(3) Physical security:

Subject to review by the Board in the event of disagreement, the Director of NSA will, in collaboration with the departments and agencies, as appropriate, formulate ^{and promulgate} minimum standards for physical security of cryptosystems and related cryptomaterial.

(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.

d. 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. 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.

e. The Director of NSA is authorized to obtain from the departments and agencies such information as he may

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

require in performing his functions, as authorized in this directive or any other directive subsequently issued.

f. 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 refer violations of such instructions outside his ^{Agency} ~~organization~~ 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

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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 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 signs, 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.

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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 (see paragraph 2-c-(1)-(d) above).

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.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~SECURITY INFORMATION~~

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.

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 or associated with the encryption or decryption of telecommunications.

j. 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.

~~CONFIDENTIAL~~