~~SECRET - SECURITY INFORMATION~~ DRAFT/26 June 1953

NSA Regulation
Number _____

POLICY AND PROCEDURE FOR DISCLOSURE OF CRYPTOGRAPHIC INFORMATION TO FOREIGN NATIONS

I. PURPOSE

1. It is the purpose of this regulation to provide general policy guidance on release of cryptographic information to foreign nations, and a uniform procedure for obtaining approval from higher authority to disclose cryptographic information to foreign nations.

II. POLICY

2. Several U. S. agencies are responsible for matters pertaining to release of information. The principal agencies through which NSA must seek approval for disclosure of cryptographic information to foreign countries are as follows:

a. The State-Defense Military Information Control Committee (S-DMICC). This Committee establishes the policy of the United States governing the disclosure of classified military information to foreign governments. S-DMICC is the final approving authority on disclosure of classified security information to foreign nations. Policies of S-DMICC must be adhered to when initiating and preparing requests for approval of release of classified cryptographic information.

b. Joint Chiefs of Staff (J.C.S.). It is the policy of the Joint Chiefs of Staff that no joint cryptographic device or publication will be made available for combined use without the approval of the Joint Chiefs of Staff.

c. United States Communications Intelligence Board (USCIB). The United States Communications Intelligence Board establishes broad policy with respect to the national COMINT effort and has certain commitments pertaining to preservation of COMINT sources. Release of cryptographic information which could have the effect of curtailing U. S. COMINT must be reviewed by USCIB.

3. Exchange of technical crypto-information with the U. K. was authorized by the Joint Chiefs of Staff following the first US/UK Communication Security (COMSEC) Conference. U.S. cryptographic information forwarded to the U. K. must be confined to the specific items authorized for discussion at the first and succeeding US/UK COMSEC conferences. Cryptoprinciples reserved for exclusive U. S. use will not be disclosed. Further developments or extensions to improve

cryptoprinciples already disclosed to the British may be disclosed provided the extension is a logical one to that cryptoprinciple, involves no new concepts, and does not use cryptoprinciples logically related to cryptoprinciples which have not been disclosed to the British. New cryptoprinciples will not be disclosed to U.K. authorities unless the following conditions are first satisfied:

a. The cryptoprinciple has been demonstrated as being feasible for development.

b. The cryptoprinciple can be used to meet an approved combined or NATO communication security requirement.

c. The Chief, Office of Communication Security, certifies that the cryptoprinciple will not be reserved for exclusive U. S. use.

4. In all cases where crypto-equipments are to be made available to the Standing Group for NATO approval or adoption, the revelation of cryptoprinciples involved should be restricted to general summaries and descriptions, and should not include specific wiring details, drawings, etc., until or unless, the equipment is in production.

5. For the purposes of this regulation, classified cryptographic information is divided into two classes, defined as follows:

Class "A"

The following types of cryptographic material and information normally will be assigned to Class "A":

a. Manual cryptographic systems for which cryptologic clearance of the user is not required. (Examples: One-time pads, double-transposition).

b. Codes (one and two part) for which cryptographic (cryptologic) clearance of the user is not required. (Examples: Bomber Codes, Map Coordinate Codes).

c. Authentication systems.

d. Devices for which cryptographic clearance of the user is not required. (Examples: Strip cipher system, NATEX).

e. Instruction pertaining to use and operation of Class "A" systems.

f. Codes and ciphers which do not require cryptographic clearance for disclosure.

g. Codes, ciphers and cryptographic techniques which are definitely established as in use or as having been in use by the recipient country(s).

Class "B"

6. The following types of cryptographic material and information normally will be assigned to Class "B":

a. Communication security equipments, usually electro-mechanical or electronic in nature.

b. Cryptoprinciples which may be incorporated in such equipments.

c. Instructions for use and operation of such equipments.

d. Cryptoprinciples of which there is reasonable doubt the recipient country has knowledge.

e. Security evaluations and cryptanalytic techniques applicable to solution of all Class "A" and Class "B" information and material.

III. PROCEDURE

7. The class into which cryptographic information is placed governs the procedure to be followed in obtaining approval for disclosure of the information. Normally, the request for disclosure of a cryptoprinciple should contain a request also for release of operating instructions and other material pertinent to operation and maintenance of the system. Coordination within NSA must include both the Chief Office of Communication Security, and the Assistant Director, Office of Production, prior to forwarding the request for disclosure to the Director for approval or signature

Class "A"

a. Disclosure of Class "A" cryptographic information may be approved by the Director. A request for approval of disclosure shall give full details including reasons for disclosure and benefits which the U. S. may expect to receive in return for the information disclosed, the nature of the material to be released, and, if pertinent, manner of reimbursement if release of material is involved and any increase in NSA COMSEC production contingent upon the release

of information. Accompanying the request will be notification to S-DMICC setting forth the information authorized by the Director for disclosure, the recipient nation or nations and the benefits expected to accrue to the U. S. by virtue of the disclosure.

Class "B"

b. In the case of Class "B" information, policies of S-DMICC, USCIB, and J.C.S. must be considered. In certain instances, prior actions by one or more of these agencies may constitute approval for release, or may, on the other hand, prohibit release. Such previous actions or decisions will be taken into account when preparing a request for disclosure. Information similar to that required for Class "A" cryptographic information will be included in the request.

c. The following considerations shall guide forwarding of requests for release through appropriate channels to the agency with final authority to approve release:

(1) While NSA COMSEC functions remain under the J.C.S., a request for release will be forwarded first to the J.C.S. for approval. If the J.C.S. approves the request will be forwarded to USCIB and will indicate that J.C.S. approval has been obtained.

(2) When J.C.S. approval for release is apparent through approval of previous actions, the request for approval will be forwarded to USCIB with a notation indicating J.C.S. approval and the circumstances of the approval.

(3) Upon receiving both J.C.S. and USCIB approval, the request will be forwarded to S-DMICC. Alternatively, the request to USCIB may request USCIB to forward the request to S-DMICC upon approval by USCIB.

e. When it is expected that cryptographic information will be introduced into the Combined Cryptographic and Security Panel of the CAN-UK-US JCECs to be considered for adoption for Combined and NATO communications, if action to obtain authority to release has not previously been initiated, such action must be initiated, with the foregoing procedure, at the time of introducing the subject into the CAN-UK-US JCECs.

TAB B

~~SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE CHAIRMAN, CENSA

SUBJECT: Disclosure of Cryptographic Information to Foreign Nations

The inclosed memorandum by the NSA members of CENSA is forwarded for consideration at the next CENSA meeting.

P. P. LEIGH, CAPTAIN, USN

for

NSA MEMBERS OF CENSA

Incl:
a/s

MEMORANDUM BY THE NSA MEMBERS OF CENSA

for

CENSA

on

DISCLOSURE OF CRYPTOGRAPHIC INFORMATION TO FOREIGN NATIONS

1. There have been several cases recently in which successful completion of actions to improve the cryptographic security of NATO and Combined (US-UK) communications have been delayed because of the necessity to obtain release approval from the State-Defense Military Control Committee (S-DMICC). In some cases it has also been necessary to receive the approval of the United States Communications Intelligence Board (USCIB) and of the Joint Chiefs of Staff (J.C.S.). In the latter instances, the Director, NSA. has usually initiated the actions necessary to obtain approval. There have been occasions also, in which the Director, NSA, has gone directly to S-DMICC requesting authority to release cryptographic information as has the JCEC on other occasions.

2. The Director NSA, is now establishing a procedure within NSA to be followed in obtaining the various approvals necessary for disclosure of cryptographic information to foreign nations. This procedure will, if accepted by the agencies exercising approving authority, provide a means of materially shortening the time usually required to obtain approval.

3. As a first step it is necessary to divide cryptographic information into two classes which are defined as follows:

Class "A" - Cryptomaterial which is used in forward or tactical echelons; has cryptoprinciples which are widely known in foreign nations; or is of such a nature that U. S. policy may not require cryptographic clearance of personnel for its use.

Class "B" - All other cryptographic information.

4. It may be noted that much of the cryptographic information which has been disclosed in the past falls into Class "A".

5. Under the proposed procedure, the Director, NSA, would authorize disclosure of cryptographic information defined as Class "A" information, and

the Director, NSA, would endeavor to obtain approval for release of Class "B" cryptographic information from the three cognizant authorities.

6. In order that items which are in Class "A" may be acted on promptly without first obtaining J.C.S. approval, the Director, NSA, proposes to forward the inclosed memorandum to the J.C.S. for approval. Similar requests will be submitted to USCIB and S-DMICC.

7. It is recommended that CENSA concur in the following actions:

a. NSA representatives on the Combined Security and Cryptographic Panel of the CAN-UK-US JCECs, prior to submitting a paper which will eventually require disclosure of cryptographic information to foreign nations will:

(1) Indicate that the information is Class "A" cryptographic information and authorized for release by the Director, NSA, or

(2) Include a statement to the effect that approval for release has been obtained from the cognizant responsible authorities.

(3) On similar papers submitted by other agencies, NSA representatives on the Combined Security and Cryptographic Panel be assigned the task of obtaining release approval and inform the Panel of this fact in a manner similar to that described above.

b. Forwarding the inclosed memorandum by the Director, NSA, to the J.C.S. for consideration.

P. P. LEIGH, CAPTAIN, USN

for

NSA MEMBERS OF CENSA

TAB C

MEMORANDUM BY THE DIRECTOR, NATIONAL SECURITY AGENCY

for the

JOINT CHIEFS OF STAFF

on

DISCLOSURE OF CRYPTOGRAPHIC INFORMATION TO FOREIGN NATIONS

References: J.C.S. 927/89

1. For the continuation of secure combined US - UK communications, and to improve the communications security of NATO forces, it is necessary from time to time to consider a U. S. cryptographic system, device or publication which might be used for this purpose. Before many of these items can be formally proposed for adoption by NATO forces, or for use in US-UK communications (which often include Commonwealth Nations not members of NATO), it is necessary that approval of the Joint Chiefs of Staff be obtained. This is required in accordance with the provisions of Joint Actions of the Armed Forces* which states that no joint cryptographic device or publication will be made available for combined use without approval of the Joint Chiefs of Staff.

2. In considering the nature of many cryptographic items for which requirements exist in NATO and in US - UK communications, a division into two classes can be made. The cryptomaterial in one of these classes can be characterized by three properties:

a. It is used in forward or tactical echelons.

b. The cryptoprinciples generally are widely known.

c. Normally cryptographic clearance is not required for access to the cryptomaterial.

3. In general, the cryptographic information in this class pertains to cryptographic systems and publications used in tactical echelons, in aircraft and in small surface craft. The items are of the following types:

Authentication systems.

Operations Codes.

Call Sign Ciphers.
Map Coordinate Codes.
Certain crypto-devices of simple nature.

4. The cryptoprinciples of these systems are generally well-known throughout the world and in some variation are used by many military forces of other countries. The security required for information encrypted by means of these systems is

*Paragraph 30813

usually for a short time only. The necessary communication security is obtained by issuing new editions of codes and making frequent changes of keying material in the case of ciphers. The communication security, therefore, is not dependent upon keeping the general nature of the system unknown but upon the keys which are used. It should be pointed out in this connection that, because of the echelon of use, capture loss of aircraft over enemy territory, etc., would lead to immediate compromise of the cryptoprinciple even if it were not already known.

5. Use of cryptographically cleared personnel for protection of crypto-material of the kind mentioned in paragraph 3 above is desirable but cannot be considered as an absolute necessity. The cost of investigating the large number of individuals in low echelons for access to such material would be very great. The time involved for investigations could affect seriously the availability of cleared personnel for communications security purposes in these echelons. Furthermore, the cryptomaterial in this class is usually based upon or closely related to well known cryptoprinciples. Consequently, the added protection afforded by a cryptologic clearance is not as important for these systems as is the case for other more advanced cryptoprinciples.

6. In recognition of the foregoing condition, Department of Defense Directive Number R-5210.2, dated 5 June 1952, authorizes NSA (AFSA) to designate certain types of cryptomaterial as non-critical from the security viewpoint and for which no cryptographic clearance is required of individuals for access to security information if various classifications is still required.

7. For cryptographic information which does not fall within the category described in the foregoing paragraphs, the provisions of Joint Action of the Armed Forces would be complied with.

8. In light of the foregoing statements, I therefore recommend that the Joint Chiefs of Staff:

a. Authorize the Director, NSA, to approve release of cryptographic material of the following types to foreign nations, subject to National policy for disclosure of classified security information:

(1) Manual cryptographic systems for which cryptologic clearance of the user is not required.

(2) Codes (one- and two-part) for which cryptologic clearance of the user is not required.

(3) Authentication systems.

(4) Cryptographic devices and machines for which cryptologic clearance of the user is not required.

(5) Other codes, ciphers, and cryptographic techniques which are definitely established as in use or as having been in use by the nation(s) involved in disclosure.

(6) Instructions pertaining to use of the foregoing cryptographic material.

b. Direct amendment of Joint Action of the Armed Forces to conform to the foregoing authorization.

9. Coordination with the Director, Communications-Electronics has been effected.

TAB D

MEMORANDUM FOR THE MEMBERS OF USCIB

SUBJECT: Disclosure of Cryptographic Information to Foreign Nations

1. There are, at present, three agencies which may be required to approve release or disclosure of cryptographic information to foreign nations These are the Joint Chiefs of Staff, USCIB, and the State-Defense Military Information Control Committee (S-DMICC).

2. At present the general national policy permits release of CONFIDENTIAL cryptographic information to Australia and New Zealand and TOP SECRET cryptographic information to the United Kingdom and Canada as necessary to permit implementation of communications agreements. In the case of all NATO countries, and of the remaining commonwealth countries, S-DMICC policy prohibits release of cryptographic information except as approved by S-DMICC in each instance.

3. The majority of the communications agreements which are being implemented, either through the CAN-UK-US JCECs or through the CECS of the Standing Group of NATO, require participation on the part of the NATO nations and the commonwealth countries. Furthermore, the majority of agreements concern the provision of tactical codes and ciphers such as aircraft codes, authentication systems, and the like, all of which come within the "Class A" category referred to in paragraph 4 below. In order for this type of material to be available when needed, and to permit training to be conducted, it is necessary to have it distributed considerably in advance of the time when the countries which require it would be participating with the U.S. in actual combat operations.

4. Generally speaking classified cryptographic information falls within one of two classes as follows:

Class "A"

The following types of cryptographic material and information normally will be assigned to Class "A":

a. Manual cryptographic systems for which cryptologic clearance of the user is not required. (Examples: One-time pads, double-transposition).

b. Codes (one and two part) for which cryptographic (cryptologic) clearance of the user is not required. (Examples: Bomber Codes, Map Coordinate Codes).

c. Authentication systems.

d. Devices for which cryptographic clearance of the user is not required. (Examples: Strip cipher system, NATEX).

e. Instruction pertaining to use and operation of Class "A" systems.

f. Codes and ciphers which do not require cryptographic clearance for disclosure.

g. Codes, ciphers, and cryptographic techniques which are definitely established as in use or as having been in use by the recipient country(s).

Class "B"

The following types of cryptographic material and information normally will be assigned to Class "B":

a. Communication security equipments, usually electro-mechanical or electronic in nature.

b. Cryptoprinciples which may be incorporated in such equipments.

c. Instructions for use and operation of such equipments.

d. Cryptoprinciples of which there is reasonable doubt the recipient country has knowledge.

e. Security evaluations and cryptanalytic techniques applicable to solution of all Class "A" and Class "B" information and material.

5. In establishing an NSA procedure for insuring that the necessary clearance actions are taken, I have received from the Joint Chiefs of Staff authority to approve release of joint cryptographic material of the Class "A" type, subject to national policy for disclosure of classified security information.

6. The material in Class "A" consists of the type of code or cipher which does not require cryptographic clearance on the part of U. S. users, contains no new cryptoprinciples but rather consists of cryptographic ideas generally known to all nations, and would cause no insecurity to U. S. communications if the cryptoprinciple is known to hostile nations. Furthermore, the NATO countries receiving such material are signatory to agreements regarding storage, accounting, and issue of cryptomaterial.

7. I, therefore, recommend, in light of the foregoing statements, that USCIB: authorize the Director, NSA, to approve release of cryptographic systems,

information, and devices to foreign nations without reference to USCIB, provided that such systems, information, and devices are Class "A" matter as defined in paragraph 4 above. The Director, NSA will keep USCIB informed of the items which he authorizes to be released and the recipient nation or nations.

TAB E

SECRET - SECURITY INFORMATION

MEMORANDUM FOR THE CHAIRMAN, S-DMICC

SUBJECT: Releasing Cryptographic Information

1. There are, at present, three agencies which may be required to approve release or disclosure of cryptographic information to foreign nations. These are the Joint Chiefs of Staff, the United States Communications Intelligence Board, and your committee.

2. At present the general national policy permits release of CONFIDENTIAL cryptographic information to Australia and New Zealand and TOP SECRET cryptographic information to the United Kingdom and Canada as necessary to permit implementation of communications agreements. In the case of all NATO countries, and of the remaining commonwealth countries, S-DMICC policy prohibits release of cryptographic information except as approved by S-DMICC in each instance.

3. The majority of the communications agreements which are being implemented, either through the CAN-UK-US JCECs or through the CECS of the Standing Group of NATO, require participation on the part of the NATO nations and the commonwealth countries. Furthermore the majority of agreements concern the provision of tactical codes and ciphers such as aircraft codes, authentication systems, and the like, all of which come within the "Class A" category referred to in paragraph 4 below. In order for this type of material to be available when needed, and to permit training to be conducted, it is necessary to have it distributed considerably in advance of the time when the countries which require it would be participating with the U.S. in actual combat operations.

4. Generally speaking classified cryptographic information falls within one of two classes as follows:

Class "A"

The following types of cryptographic material and information normally will be assigned to Class "A":

a. Manual cryptographic systems for which cryptologic clearance of the user is not required. (Examples: One-time pads, double-transposition).

b. Codes (one and two part) for which cryptographic (cryptologic) clearance of the user is not required. (Examples: Bomber Codes, Map Coordinate Codes).

c. Authentication systems.

d. Devices for which cryptographic clearance of the user is not required. (Examples: Strip cipher system, NATEX).

e. Instruction pertaining to use and operation of Class "A" systems.

f. Codes and ciphers which do not require cryptographic clearance for disclosure.

g. Codes, ciphers, and cryptographic techniques which are definitely established as in use or as having been in use by the recipient country(s).

Class "B"

The following types of cryptographic material and information normally will be assigned to Class "B":

a. Communication security equipments, usually electro-mechanical or electronic in nature.

b. Cryptoprinciples which may be incorporated in such equipments.

c. Instructions for use and operation of such equipments.

d. Cryptoprinciples of which there is reasonable doubt the recipient country has knowledge.

e. Security evaluations and cryptanalytic techniques applicable to solution of all Class "A" and Class "B" information and material.

5. In establishing an NSA procedure for insuring that the necessary clearance actions are taken, I have received from the Joint Chiefs of Staff authority to approve release of joint cryptographic material of the Class "A" type, subject to national policy for disclosure of classified security information.

6. The material in Class "A" consists of the type of code or cipher which does not require cryptographic clearance on the part of U. S. users, contains no new cryptoprinciples but rather consists of cryptographic ideas generally known to all nations, and would cause no insecurity to U. S. communications if the cryptoprinciple is known to hostile nations. Furthermore, the NATO countries receiving such material are signatory to agreements regarding storage, accounting, and issue of cryptomaterial.

7. I, therefore, recommend in view of the foregoing statements that the State-Defense Military Information Control Committee authorize the Director, National Security Agency, to authorize release of cryptographic systems, information and devices necessary to implement communication agreements provided that such systems, information and devices are Class "A" material

as defined in paragraph 4 above. The Director, NSA, will keep the S-DMICC informed of the items which he authorizes to be released and the recipient nation or nations.