

19 March 1953

APPENDIX B

PRINCIPLES OF SECURITY AND DISSEMINATION

INTRODUCTION

1. These principles shall be the basis of all regulations for the security and dissemination of Communications Intelligence issued by or under the authority of USCIB or LSIB and other appropriate authorities of the Governments of the two parties. The scope and phrasing of such regulations may vary in accordance with requirements of the parties, agencies, departments, and ministries to whom they are designed to apply, but all shall be in accord with these basic principles in every respect and shall observe the standards herein as a minimum. As an aid to uniform interpretation, each party shall forward all pertinent Board regulations and directives to the other for information.

2. It is recognized that, while the following principles are in general of universal application, changing conditions or emergencies and, in particular, the outbreak of general hostilities may require modification to ensure that the maximum operational benefit consistent with security is derived from communications intelligence.

DEFINITIONS AND CATEGORIES

3. Communication Intelligence (COMINT) is the name given to all processes involved in, and intelligence information and technical material resulting from, the interception and study (a) of foreign communications passed by wire, radio, and other electromagnetic means (except press, propaganda, and public broadcasts) and (b) of selected foreign communications sent by non-electromagnetic means. [See NOTE 1.]

4. There are two types of COMINT: Crypt Intelligence and Traffic Intelligence [See NOTE 2]. They are defined as follows:

a.

b. Traffic Intelligence is that COMINT which results from traffic analysis (e.g. the study of call-signs, message headings, procedure signals, volume of traffic, precedences, D/F bearings, and other aids such as ) and from plain texts, i.e., information produced by all means short of the actual crypt-analysis of intercepted communications.

5. For purposes of security handling and control COMINT is divided into Categories and Sub-Categories.

a. COMINT is divided at the present time to three Categories:

Category III COMINT

Category II COMINT

Category I. COMINT

EO 3.3(h)(2)  
PL 86-36/50 USC 3605

b. COMINT is placed in appropriate Categories as mutually agreed by USCIB and LSIB from time to time.

c. As mutually agreed by USCIB and LSIB, separate Sub-Categories of COMINT may be established within Categories III and II in order to permit differentiation in the processing, dissemination, exchange or use of material.

6. Category III COMINT is that COMINT for which the protection of source or content is the overriding consideration and which must, therefore, be given the highest degree of security protection. In general, it will include:

a. Crypt Intelligence except that specifically included in other Categories.

b. Special Weather Intelligence.

c. Traffic Intelligence involving call-signs or message headings encrypted in codes or ciphers of high security gradings as specified and mutually agreed by USCIB and LSIB.

d. Other Traffic Intelligence as specified and mutually agreed by USCIB and LSIB.

7. Category II COMINT is that COMINT for which the protection of source or content is not always the overriding consideration and for which a less rigid standard of security is considered an acceptable risk. In general, it will include:

- a. Traffic Intelligence not specifically included in other Categories.
- b. Crypt Intelligence involving solution of codes, ciphers and special systems of lower security as specified and mutually agreed by USCIB and LSIB.

8. Category I COMINT is that COMINT which may be subject to the least stringent security restrictions and which may require more extensive dissemination in order to provide for effective utilization. In general, it will include certain types of low level COMINT as specified and mutually agreed by USCIB and LSIB.

ASSIGNMENT OF COMINT TO CATEGORIES

9. In assigning COMINT to a Category, the following general criteria will be considered:

- a. The intelligence value of its content.
- b. The difficulty of solution or intercept to include:
  - (1) Sensitivity of techniques employed in solution and exploitation.
  - (2) Sensitivity of source of intercept.
  - (3) Inter-relationships between cryptographic systems.
- c. Cryptographic sophistication of the country originating the traffic involved.
- d. Security grading given to contents by the country originating the traffic involved.
- e. The advantage to be gained versus the risk of loss by utilization under a given Category, including:

19 March 1953

- (1) The value of extending the dissemination of certain COMINT to permit essential use of the operational intelligence contained therein.
- (2) The capability of certain Third Party COMINT groups to exploit the COMINT in question with the attendant security risks beyond the direct control of U.S. and U.K. authorities.
- (3) The value of providing technical guidance or COMINT information to Third Party COMINT activities to insure receipt from them of unique intercept and critical COMINT information not otherwise available.

10. In assigning COMINT to the lower Categories the following additional factors will be considered:

- a. A system or class of COMINT, once downgraded, may not effectively be upgraded.
- b. The distinction between Category I on the one hand and the higher Categories on the other is that the former does not require codeword protection, whereas the latter do.

11. USCIB and LSIB shall have prepared and maintained in current status mutually agreed lists to indicate COMINT placed in the several Categories and in such Sub-categories as may be established.

CLASSIFICATION AND CODEWORDS

12. Category III COMINT shall be classified TOP SECRET and shall be designated by a distinctive codeword agreed between USCIB and LSIB and replaced every two years. In the event that USCIB and LSIB agree that positive security advantages will be obtained by earlier change then such change shall be made and a new period of two years shall be in effect from that date.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

19 March 1953

13. Category II COMINT shall be classified SECRET and shall be designated by a distinctive codeword agreed between USCIB and LSIB and replaced every two years. In the event that USCIB and LSIB agree that positive security advantage will be obtained by earlier change then such change shall be made and a new period of two years shall be in effect from that date.

14. Category I COMINT shall be classified not lower than CONFIDENTIAL and shall not be designated by a codeword.

15. Sub-categories. Whenever a Sub-category is established within Categories III or II COMINT, it shall be designated by a separate or auxiliary codeword agreed from time to time between USCIB and LSIB.

16. Technical material pertaining to COMINT shall bear the classification and codeword appropriate to the most highly classified and sensitive Category or Sub-category of COMINT to which it relates and shall be handled accordingly.

17. Documents which reveal actual success, progress, or processes in the production of COMINT shall bear the classification and codeword appropriate to the most highly classified and sensitive Category or Sub-Category of COMINT to which they relate and shall be handled accordingly, even though such documents may not reveal COMINT as such.

18. Raw traffic (i.e., intercepted traffic showing no evidence of processing for COMINT purposes beyond sorting by clear address elements, elimination of unwanted messages and the inclusion of a case number and/or an arbitrary traffic designator) shall be classified not lower than CONFIDENTIAL and need not be designated by a codeword.

19. Codewords. When used as such, the codewords which designate Categories III and II COMINT, and the Sub-Categories which may be established within these Categories shall bear the TOP SECRET classification according to the Category. These codewords and their implications shall not be made known to non-indoctrinated persons, nor shall these codewords be used in their codeword sense in the presence of non-indoctrinated persons.

SECURITY

19 March 1953

20. Conservation of COMINT sources is of supreme importance. It is essential, therefore, that the production, exploitation, and dissemination of COMINT, and of all related or resultant information, be strictly controlled and the dissemination appropriately limited. The physical security of related documents is not alone sufficient; it is essential that all reference to the existence of COMINT, either direct or indirect, be avoided except among those to whom the knowledge is necessary for the proper performance of their duties. These provisions shall apply to any intelligence which, in whole or in part, includes information which can be traced solely to COMINT sources.

21. There is no time limit for the safeguarding of COMINT as defined herein. It is of the utmost importance that complete and absolute silence on all COMINT matters be maintained by those who have ever been indoctrinated for COMINT. If, at any time, matter referring to COMINT is broadcast or published, even though by prominent people or those in authority, this does not in any way free those other persons who are, or ever have been indoctrinated for COMINT from their continuous obligation to maintain silence.

22. Except as agreed by USCIB or LSIB, all persons to be assigned to duties involving COMINT shall be the subject of security investigation and clearance. As an aid to the uniformity of investigations and clearances, and to promote adequate minimum standards, each party shall inform the other of the standards prescribed by it for this purpose.

23. All persons to be assigned to duties involving Categories of COMINT other than Category I shall be indoctrinated (i.e., instructed as to the nature of COMINT and the security regulations and practices which govern the handling of COMINT material and COMINT activities). Recipients of Category I COMINT only will not be indoctrinated. Producers of Category I COMINT only need not necessarily be indoctrinated.

19 March 1953

a. Knowledge of specific Categories or Sub-Categories of COMINT shall be made available to indoctrinated persons solely on the basis of their "need to know".

b. Every effort shall be made to restrict the number of persons indoctrinated for COMINT to the essential minimum.

c. It shall be permissible for persons who have access only to a less sensitive Category or Sub-Category of COMINT to work within Agencies or Centers in which there are located other persons engaged in the production or exploitation of a more sensitive Category or Sub-Category of COMINT, only so long as due precaution shall be taken (by providing segregated, secure areas or otherwise) to ensure that the activities and knowledge of such persons are confined to the COMINT material and activities to which they have access.

24. Under extraordinary conditions, as determined by USCIB or LSIB, it may be essential for an individual to take up duties involving COMINT before the requisite investigation can be completed. In such cases, the person concerned may be suitably indoctrinated on the authority only of senior officers or officials as designated by the respective parties. In all such cases, steps shall be taken to ensure that security investigations and clearances are completed as soon as possible after indoctrination.

25. Each Party shall ensure that complete lists of indoctrinated persons are maintained.

26. USCIB and LSIB shall keep each other fully informed of the approximate number of indoctrinated persons in each of the Departments, Ministries, Agencies, and Offices receiving COMINT, by Category of Sub-Category where applicable.

27. No national of one party shall be permitted access to the COMINT agencies or to the Categories III and II COMINT of the other Party,

19 March 1953

unless he has been approved by his parent agency or Board and has been properly indoctrinated. Such access shall be limited to the Categories or Sub-Categories of COMINT agreed by his parent agency or Board.

28. Every effort shall be made to ensure that no person who has a knowledge of current value about COMINT, such that his capture or interrogation could be a substantial risk to the security of COMINT, shall be assigned to or engage in activities of a hazardous nature.

29. "Hazardous activities" are those which place a person in a position where he runs a substantial risk of being captured or otherwise subjected to interrogation, e.g.:



30. In applying these principles persons who are or have been indoctrinated will be divided into four groups:

- a. Producers of Category I COMINT who have no knowledge of other Categories are classed as Group A. They may be assigned to hazardous activities only on the authority of senior officers. (No restrictions are applied to the recipients or non-indoctrinated producers of Category I COMINT only).

EO 3.3(h)(2)  
PL 86-36/50 USC 3605

19 March 1953

- b. Individuals who have knowledge of current value about Category II COMINT are classed as Group B. They may be assigned to hazardous activities only after six months separation from such material.
- c. Individuals, other than those specified in sub-paragraph d below, who have knowledge of current value about Category III COMINT are classed as Group C. They may be assigned to hazardous activities only after a separation of one year or longer from this type of information.
- d. Individuals with precise knowledge of COMINT processing techniques, competence, or potential, regarding the more sensitive Category III COMINT material are classed as Group D. They shall not be assigned to hazardous activities at any time.

31. The provisions in paragraphs 28, 29 and 30 shall be applied only by senior officers and officials at a level to be established by USCIB or LSIB. Exceptions shall be authorized only after careful consideration in each instance of the advantages to be gained, as opposed to the risk involved. In considering exceptions to sub-paragraph 29d, the protection offered by diplomatic status should not automatically be considered sufficient, but should be assessed in the light of the particular circumstances involved. Any exception in the case of Group D personnel must receive prior approval by the Board concerned. The considerations relevant to COMINT personnel serving with COMINT units in exposed areas are dealt with in Annexure B2. All possible action shall be taken to discourage or prevent any individual with a knowledge of current value about COMINT from engaging in hazardous activities (as defined in paragraph 29 above) in any unofficial capacity at any time.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

19 March 1953

32. Except as implicitly involved in the operation of paragraphs 35, 41 and 42 below, Categories III and II COMINT shall remain exclusively in the custody of indoctrinated persons, secure from examination by non-indoctrinated persons.

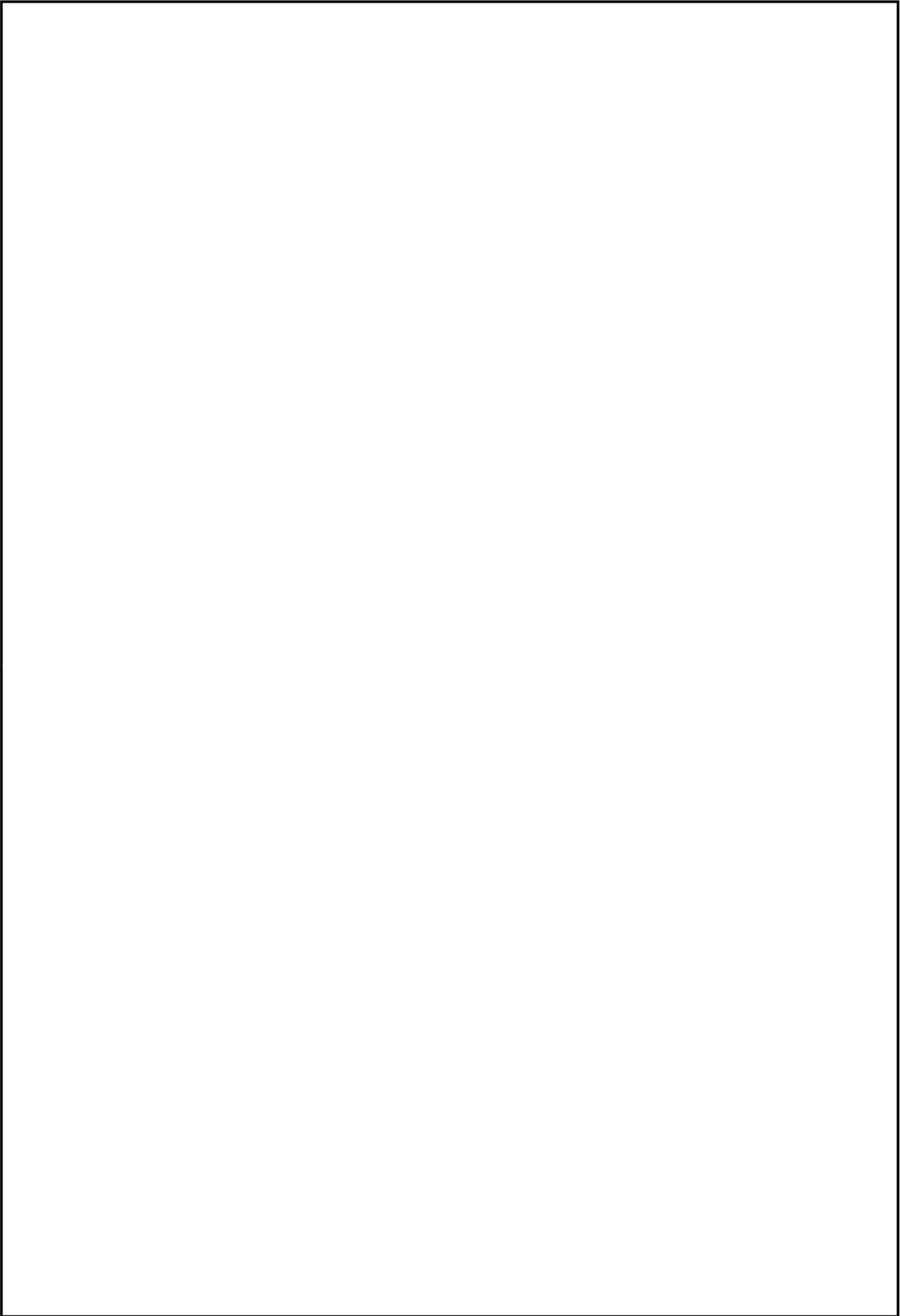
DISSEMINATION

33. The basic principle governing the dissemination and use of COMINT is the "need to know". Each item of COMINT shall, therefore, be made known only to those individuals who require it in the performance of their duties and, except as specifically provided in paragraphs 35, 36 and 37 below, are indoctrinated and authorized to have access to the particular Category or Sub-Category of COMINT to which such item appertains.



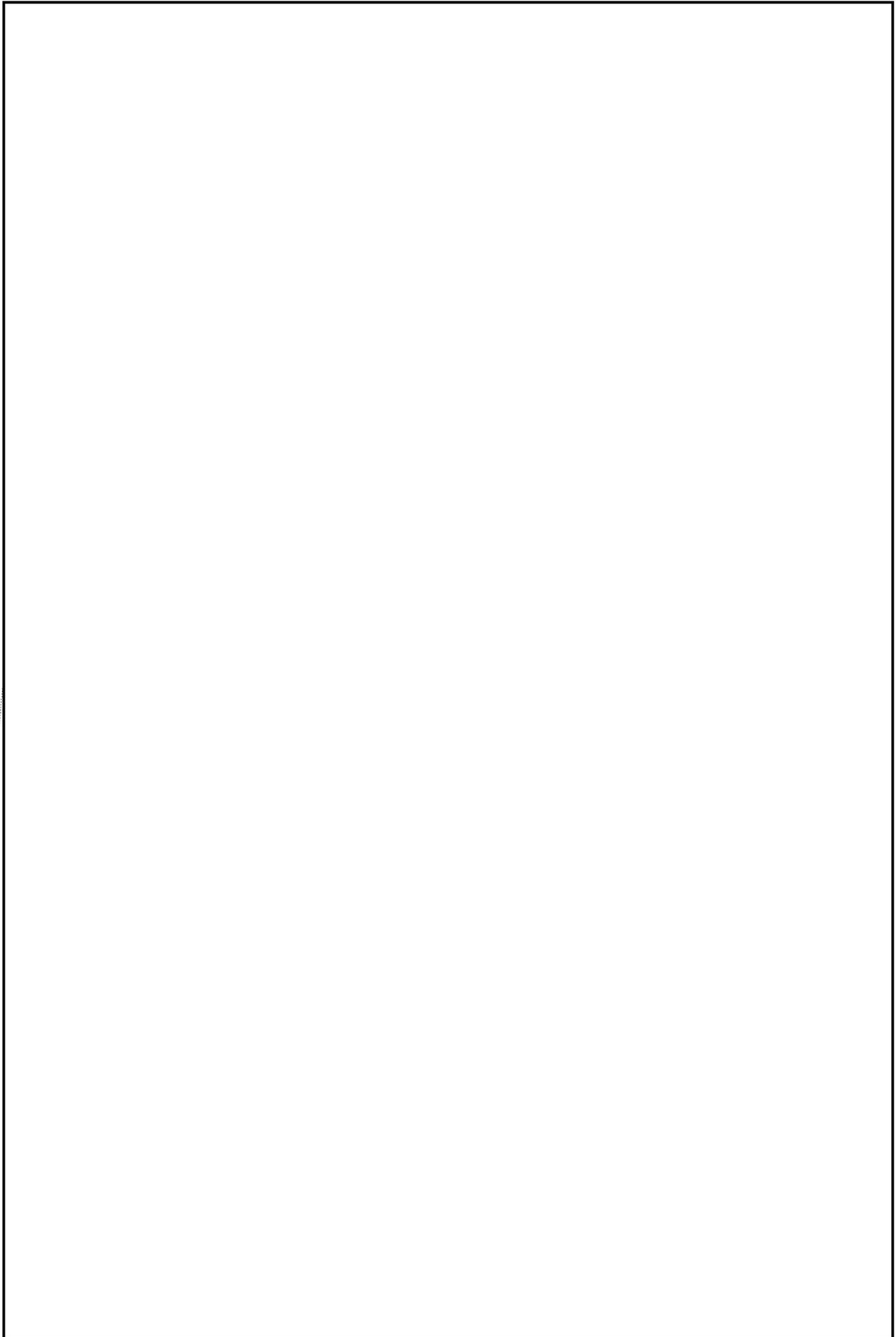
EO 3.3(h)(2)  
PL 86-36/50 USC 3605

19 March 1953



EO 3.3(h) (2)  
PL 86-36/50 USC 3605

19 March 1953



19 March 1953



36, Category I COMINT may be disseminated in accordance with the normal practice of each Party as regards intelligence materials of similar classifications. However, it may not be passed to Third Party recipients except as provided in paragraph 37 below, and must be handled accordingly. It is recognized that this dissemination will involve loss of control by COMINT authorities, but every effort shall be made to ensure that the following provisions are enforced to the maximum extent possible.

- a. Whenever Category I COMINT is to be transmitted by a means exposed to interception, it shall normally be transmitted in an appropriate cryptographic system. It may be transmitted in plain language only when there is no suitable means of secure communication available and when there is an urgent operational need to do so. Whenever possible such plain language transmissions shall be in the form of operational orders so worded that the subject matter cannot be traced specifically to its COMINT origin.

EO 3.3(h) (2)  
PL 86-36/50 USC 3605

19 March 1953



37. Category I COMINT may be disseminated to Third Party recipients under the following conditions:

a. In COMINT arrangements with Third Parties, Category I COMINT may be released to these Third Parties in accordance with the provisions of Appendix P.

b. During active hostilities or in the case of an emergency involving a matter of importance to the national security of either Party, Category I COMINT may be disseminated to nationals of Third Parties who are engaged directly with the U.S. or U.K. in these hostilities or are allied directly with the U.S. or U.K. in dealing with the emergency concerned. The determination of a requirement to make this exception and the authority to grant this exception shall lie only with senior officers or officials at a level to be established by USCIB or LSIB.

38. In the event that either Party produces individual items of COMINT which, by reason of the extreme sensitivity of their source or content shall be given a more limited dissemination than would normally be given to the Category or Sub-Category of COMINT within which they fall, it will be for the originating party to indicate the nature of the special handling desired and to request that the other Party afford similarly limited dissemination.

39. Category III and II COMINT shall never under any circumstances or in any form be disseminated to any Ministry, Department, Agency, Organization, Office, or individual from which or from whom it might reasonably be expected to find its way, officially or extra-officially, into the possession of any person or group who could use it for commercial competition or commercial gain or advantage.

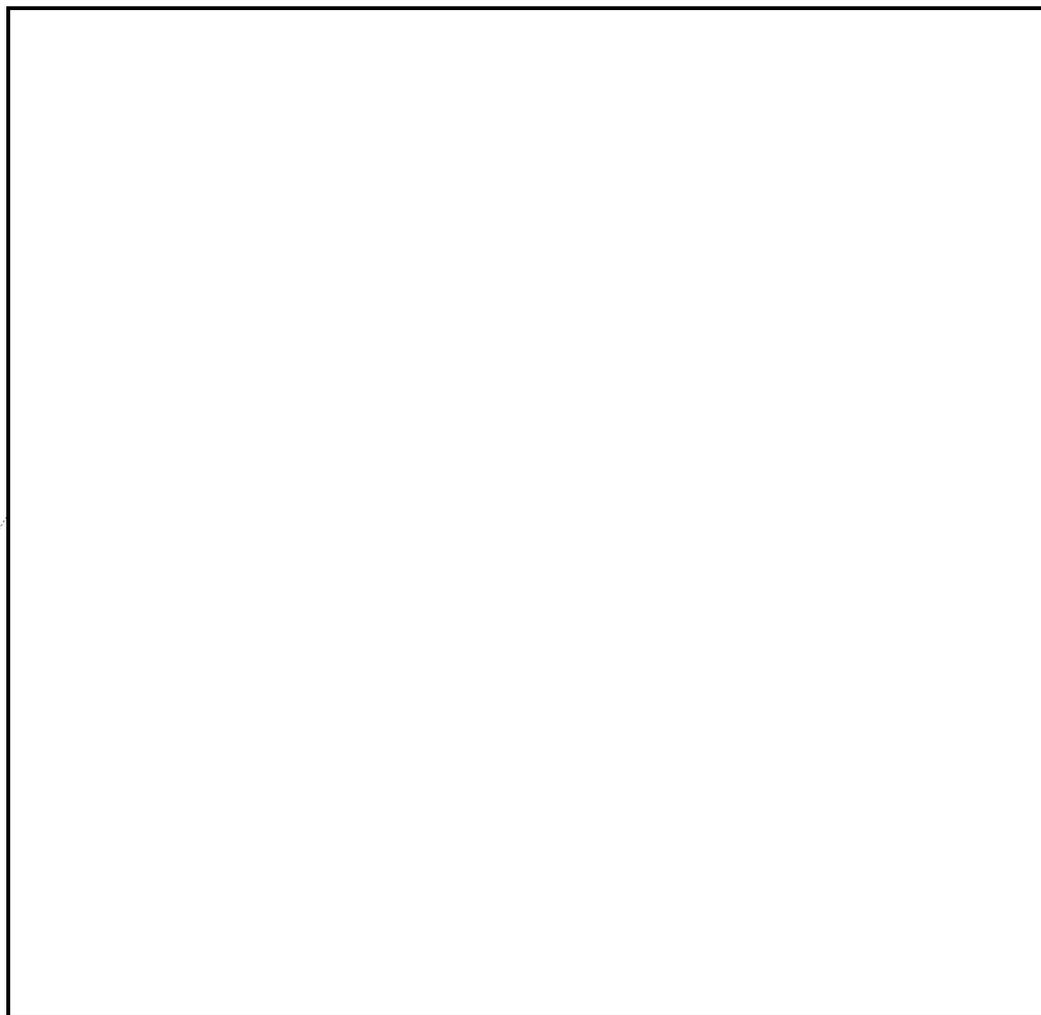
~~TOP SECRET CANOE - SECURITY INFORMATION~~

19 March 1953

PROCEDURES

40. The appropriate classification and codeword shall:
- a. Appear on every sheet of paper which contains or discloses Category III or II COMINT or a Sub-Category thereof, technical material pertaining to these Categories and Sub-Categories and documents which reveal actual success, progress or processes in their production. Except as provided in paragraph 35 above, this rule applies to maps and charts on which are plotted data and information derived from these categories of COMINT.

b.



EO 3.3(h)(2)  
PL 86-36/50 USC 3605

19 March 1953

41. Category III COMINT and related technical material shall not be transmitted in plain language except as follows:

- a. Sealed, by safehand channels, over routes specifically approved by USCIB or LSIB. Each Board shall inform the other of all approved routes involving transport across territory of a third party, the approval of such routes to be held to the necessary minimum.
- b. Over landlines specifically approved in each instance by USCIB or LSIB.
- c. Over completely protected local communication systems exclusively internal to agencies or offices producing or utilizing COMINT.

42. Category II COMINT and related technical material shall not be transmitted in plain language except as provided in paragraph 41 above, or by protected postal channels internal to, or under exclusive control of the US, the UK, or other collaborating British Commonwealth countries.

43. Category I COMINT and related technical material should be transmitted by COMINT channels wherever possible, but may be transmitted by conventional channels used for intelligence materials of similar classification. It shall not be transmitted in plain language by a means exposed to interception, except as provided in sub-paragraph 36a above.

44. Raw traffic may be transmitted in plain language as provided in paragraphs 41 and 42 above. Raw traffic classified CONFIDENTIAL may also be transmitted in accordance with the normal procedure for this classification, except that when transported across the territory of the country originating the traffic, it shall be with the express sanction of USCIB or LSIB. This sanction will be granted only in cases of compelling need.

19 March 1953

45. Except as provided in paragraph 35 above:

- a. Category III COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects.
- b. Category II COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects, those listed in paragraph a above, or in the most secure cryptographic channel available.
- c. However, in the case of cryptographic systems mutually approved for the purpose, the transmission of COMINT related technical matters and raw traffic over the same channel is authorized, provided that such channels are reserved for these subjects exclusively.

46. In order to facilitate a concerted effort directed toward the determination and assessment of the causes and effects of known or presumed COMINT compromises or losses, it is agreed that:

- a. Whenever any breach of its COMINT security regulations or any other circumstance which in fact has, or can be presumed to have, compromised COMINT or COMINT codewords, or to have revealed COMINT successes to unauthorized persons, becomes known to either Party, it shall inform the other by means of a report embodying the pertinent facts and conclusions in each case, except that when the Party concerned concludes that there is a good reason to believe that such compromise or revelation has not reached and will not, in fact, reach foreign nationals, no report need be made to the other Party.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

19 March 1953

- b. Whenever a significant change occurs in foreign cryptographic or communications security, the Party discovering such change shall notify the other. Each Party shall then analyze and assess the known and suspected circumstances having a bearing upon the change; these analyses and assessments shall be exchanged by the Parties; and each Party shall thereafter keep the other fully informed of any additional information bearing upon the case.

19 March 1953

Notes to Appendix B

EO 3.3(h)(2)  
PL 86-36/50 USC 3605

Note 1 Throughout this Appendix:

a. "Foreign communications" are understood to mean those of the Government, or of any military, Air or Naval force, faction, party, department, agency or bureau of a foreign country, or any person or persons acting or purporting to act therefor, and shall include  and private communications originated by nationals of a foreign country which may contain information of military, economic, political, or counter intelligence value. "Foreign country" is understood to include all countries, whether or not their governments are recognized by the US or the UK, excluding only the US and the British Commonwealth of Nations.

b. "Technical material" is understood to mean data concerning:

- (1) cryptographic systems,
- (2) communications procedures and methods,
- (3) methods and equipment, as used in or designed for  
COMINT processes,

and information related to any of the above.

c. "Communications intelligence" does not include the interception and study of non-communications transmissions. The term Signal Intelligence (Sigint) (as used by the UK) includes both COMINT and the interception and study of non-communications transmissions. These transmissions are outside the scope of this Appendix.





Note 3 Paragraph 3<sup>4</sup> shall be so interpreted as to allow:

a. The use of COMINT by indoctrinated persons in the preparation of National Intelligence Estimates, JIC appreciations and similar documents issued without COMINT codewords, as specified by either party, provided the statements contained in them are so generalised that they cannot be traced to a particular item of COMINT or to their COMINT origin. Specific COMINT detail must be restricted to supporting papers carrying the COMINT codeword.

