

~~TOP SECRET FROTH~~

29

~~TOP SECRET FROTH~~

(Revised 27 March 1953)

APPENDIX BPRINCIPLES OF SECURITY AND DISSEMINATIONINTRODUCTION

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 CRC 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. Communications 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. Crypt Intelligence is that COMINT which results from crypt-analysis including the solution of speech and facsimile security systems.

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 RFP) and from plain texts, i.e., information produced by all means short of the actual cryptanalysis 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 into three Categories:

Category III COMINT

Category II COMINT

Category I COMINT

b. COMINT is placed in appropriate Categories as mutually agreed by USCIB and CRC from time to time. The assignment of COMINT to Categories, pursuant to this sub-paragraph and other provisions of this Appendix, shall

- 1 -

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~TOP SECRET FROTH

be made by the party performing the analysis and processing involved, except that, where these are performed by both parties, assignment to Categories shall be as mutually agreed.

c. As mutually agreed by USCIB and CRC, 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 CRC.

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

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 CRC.

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 CRC.

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.

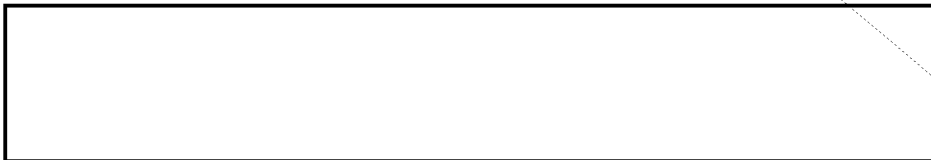
~~TOP SECRET FROTH~~EO 3.3(h)(2)
PL 86-36/50 USC 3605~~TOP SECRET FROTH~~

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:

- (1) The value of extending the dissemination of certain COMINT to permit essential use of the operational intelligence contained therein.



- (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 CRC 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 CRC and replaced every two years. In the event that USCIB and CRC 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.

13. Category II COMINT shall be classified SECRET and shall be designated by a distinctive codeword agreed between USCIB and CRC and replaced every two years. In the event that USCIB and CRC 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 CRC.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

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, need not be designated by a codeword and is understood not to be any specific Category of COMINT.

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 or 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

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 GRC, 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, including intercept operators, 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

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

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.

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 CRC, 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 CRC 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 or 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, 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.:

a. Duties behind enemy lines, or in-shore operations off an enemy or Iron Curtain country.

b. Flights over enemy or Iron Curtain territory unless on recognized corridor routes.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

c. Raids, minor formation attacks, underwater demolition operations, and service with a unit of formation forward of Division HQ.

d. Duty in or visits to Iron Curtain countries and also other areas where from time to time local conditions are considered to involve an unacceptable risk.

e. Transit through the Soviet Zones of Germany and Austria unless in authorized military or diplomatic transport on regular routes.

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.)

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 subparagraph 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 CRC. 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 subparagraph 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.

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.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~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.

34. Categories of COMINT other than Category I, including any intelligence which in whole or in part can be traced solely to those categories, shall be disseminated only to persons who are indoctrinated and authorized to have access to such material. No action based on such material shall be taken in the absence of a suitable cover to which the action can be attributed without connection with these COMINT sources. A suitable cover must include either the existence of similar intelligence from other sources or an actual situation wherein the intelligence itself can be attributed beyond reasonable doubt by non-indoctrinated persons (including foreign nationals) to other sources or events, such as appropriate reconnaissance during military hostilities [See NOTE 3].

35. There shall be no exceptions to paragraph 34 except as listed below. In making these exceptions, a studied effort shall be made to ensure that, insofar as possible, information or action cannot be attributed to COMINT sources and a minimum number of non-indoctrinated persons is involved. Such persons are to be given only the minimum information needed. Save as specifically provided for within mutually agreed arrangements affecting third parties (see sub-paragraph 35c below) COMINT codewords shall not be used and necessary communications shall be so worded that the subject matter cannot be traced specifically to COMINT, names, times, positions, and other data identical with that from original texts being omitted or carefully disguised wherever possible. If such communications are to be transmitted by means exposed to interception, they shall be encrypted in the most secure cryptographic channel available.

a. Technical instructions based on COMINT of any Category may be issued to non-indoctrinated intercept operators, including D/F, RFP operators and the like, without use of the appropriate codeword if in such form and of such nature as neither to give indication nor to permit reasonable deduction of the COMINT origin, and provided they are essential to the tasks of those concerned.

b. Weather forecasts and conclusions based in whole or in part on the analysis of maps, on which Special Weather Intelligence [See NOTE 2] has been plotted, may be issued to non-indoctrinated persons without use of the appropriate codeword, but only in such form as to give no indication of COMINT origin.

c. In COMINT arrangements with third parties, Category III and II COMINT may be released to these Third Parties in accordance with the provisions of mutually agreed arrangements affecting third parties.

d. In the case of an extreme emergency in which there is an imminent threat to the vital, national interests of either party, Category III and II COMINT may be disseminated to non-indoctrinated persons and action may be taken. The determination of a case of extreme emergency which justifies making this exception shall be made only at the highest level as established by USCIB or CRC. Whenever action is taken under this paragraph both Boards shall be notified. If Third Parties are involved or are likely to be involved, the prior agreement of both Boards shall be obtained whenever time permits.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

e. In the case of an emergency involving a matter of importance to the national security of either party, Category II COMINT may be disseminated to non-indoctrinated persons and action may be taken. The determination of a matter of sufficient importance to justify making this exception shall be made only by senior officers or officials at a level to be established by USCIB or CRC. Whenever action is taken under this paragraph both Boards shall be notified. If Third Parties are involved or are likely to be involved, the prior agreement of both Boards shall be obtained whenever time permits.

f. The exceptions described in sub-paragraphs 35d and 35e above shall be made only upon a determination that the advantages to be gained clearly justify the risk of compromise of the COMINT source and the extent of the loss which would probably follow such a compromise. In making this determination, due regard shall be given to:

- (1) The availability of suitable cover.
- (2) The relative value of the particular COMINT source involved and the possibility that its compromise may lead to the loss of other COMINT sources, particularly those which are more valuable.
- (3) The possible repercussions on current and future operations and also on other commands and areas.

g. When it is essential to operations directly related to the national security of either party, action may be taken based on such Category II plain text as agreed by both parties, and such COMINT may be included in documents and operational directives not carrying a COMINT codeword, provided that there is adequate reason why the recipients should not be indoctrinated. This exception shall be made only under the following conditions:

- (1) All precautions must be taken to ensure that COMINT does not thereby come to the knowledge of Third Parties..
- (2) The advantages to be gained are sufficiently great to justify the risk to the COMINT source.
- (3) The information could reasonably be attributed by non-indoctrinated persons (including foreign nationals), to other sources-agent, attache-defector, and the like.
- (4) The COMINT origin of the information is not stated. Whenever possible and plausible the information shall be specifically attributed to other sources.
- (5) The determination of a matter of sufficient importance to justify these exceptions shall be made only by senior officers or officials at a level to be established by USCIB or CRC.
- (6) USCIB or CRC shall be notified by the Agency concerned when action is taken under this sub-paragraph.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

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.

b. In taking action based on Category I COMINT care shall be taken not to risk the COMINT source unnecessarily. Whenever possible, efforts shall be made to devise a suitable cover.

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 mutually agreed arrangements affecting Third Parties.

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 [] in these hostilities or are allied directly with the U.S. or [] 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 CRC.

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.

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

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~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. Be encrypted in the text of every encrypted communication conveying Category III and II COMINT and appear in plain language at the head of the decrypted version. This rule shall apply in all instances except as provided in paragraph 35 above and under the following conditions:

- (1) COMINT agencies may, without encrypting the appropriate codeword in the encrypted text, transmit TOP SECRET and SECRET technical matter over cryptographic channels or ciphers expressly and exclusively provided for such technical matters.
- (2) COMINT agencies and intercept or D/F stations may, at the discretion of the officer in charge and after full consideration of the risks involved to the source, omit the classification and the appropriate codeword from its work-sheets and similar documents used exclusively within each agency or station. The classification may be omitted from raw traffic passed between agencies or from intercept and D/F stations to agencies.

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 CRC. 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 CRC.

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, and Canada 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.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

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 CRC. This sanction will be granted only in cases of compelling need.

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.

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.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~EO 3.3(h)(2)
PL 86-36/50 USC 3605Notes to Appendix BNote 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 commercial 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 [redacted]

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. For purposes of this Appendix "Communications intelligence" does not include the interception and study of non-communications transmissions.

Note 2 In order to facilitate and control the dissemination of COMINT concerning weather to meteorological (met) authorities and to distinguish it from other Crypt and Traffic Intelligence, with which these authorities are not concerned, such COMINT is termed Special Weather Intelligence.

a. "COMINT concerning weather" is that COMINT derived from Communications which contain meteorological data, hydro-meteorological data and/or information concerning meteorological organizations and activities. It does not include published broadcasts of the World Meteorological Organization (WMO) transmitted in unenciphered WMO codes.

b. "Special Weather Intelligence" is that COMINT concerning weather which is disseminated to met organizations, except that:

- (1) COMINT concerning weather which would normally be disseminated to met organizations may, when derived from selected communications as specifically agreed between USCIB and CRC, be treated as Crypt Intelligence.
- (2) COMINT concerning weather which is derived from Category I COMINT sources (see paragraphs 5 and 8) and disseminated to met organizations may be treated either as Special Weather Intelligence or as Category I Crypt or Traffic Intelligence as appropriate.
- (3) COMINT concerning weather which is disseminated to both met and non-met organizations may, in the latter instance, be treated as Crypt or Traffic Intelligence as appropriate.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

Note 3 Paragraph 34 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.

b. Target information derived from COMINT, for which there is suitable cover, to be entered on maps and in target folders issued without COMINT codewords, but only in such form as does not indicate or reveal the COMINT origin.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~APPENDIX BANNEXURE B1THE ASSIGNMENT OF COMINTTO CATEGORIES AND SUB - CATEGORIES

1. This Annexure delineates the basis for (a) the establishment of Sub-Categories, (b) the assignment of COMINT to Categories and Sub-Categories, (c) the classification of COMINT assigned to Category I and (d) the application of codewords to designate Sub-Categories, as provided in paragraphs 5c, 5-8, 14 and 15 of Appendix B respectively. This Annexure is not intended to specify or accomplish the detailed categorization of all COMINT. However, along with the criteria described in paragraphs 9 and 10 of Appendix B, it governs the preparation and maintenance of current, mutually agreed lists, which are required under paragraph 11 of Appendix B, to indicate the precise assignment of all COMINT to Categories and Sub-Categories.

2. Category I shall contain:

- a. Traffic intelligence relating to D/F mission assignments, bearing reports and fix reports (i.e.: target frequencies, call-signs, "piped signals", other signal information, bearings and fixes), provided that no interpretations of complex changing call-sign systems are included. This material shall normally be classified CONFIDENTIAL.
- b. Plain-text tactical or operational traffic provided that no interpretations of complex changing call-sign systems, enciphered map references, or results of advanced traffic analysis are included. This material shall include local procedural and local grid and zone systems used for artillery direction, tactical control and movement of front line units, early warning and exercise of tactical combat control of aircraft. This material shall normally be classified CONFIDENTIAL.
- c. Traffic Intelligence or Crypt Intelligence from analysis of radar tracking reports and visual observation reports as found in tactical or operational traffic, provided that enciphered aircraft type designations or interpretations of complex changing call sign systems are not included. Inclusion of local grid or zone references, local procedural codes used for brevity and plain-text interspersed with cover words is permissible. This material shall normally be classified CONFIDENTIAL.
- d. Crypt Intelligence from naval tactical maneuvering codes, when used as such, and from jargon codes. This material shall normally be classified CONFIDENTIAL.
- e. COMINT concerning weather which is derived from Category I COMINT sources, as referred to in NOTE 2b to Appendix B, includes only that COMINT described in sub-paragraphs 2b and 2c above.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~EO 3.3(h)(2)
PL 86-36/50 USC 36053. Category II shall contain

- a. Traffic Intelligence (including freely available privacy and brevity systems such as commercial codes) except where specifically assigned to other Categories. Category II plain-text which qualifies for exceptional handling under paragraph 35g of Appendix B shall include only such of the following as is not assigned to Category III under subparagraphs 4d and 4e below:

--

- b. Crypt Intelligence specifically assigned on the basis of crypto-systems. USCIB and CRC shall have supplementary lists of all cryptosystems mutually adjudged suitable for inclusion in this Category kept jointly in current status by their respective technical groups. These lists shall be based upon the criteria in sub-paragraphs 9a, b, c, and d, and paragraph 10 of Appendix B. Either Party may, after consideration of advantages and risks as provided in subparagraph 9e of Appendix B, assign any crypto-system currently so listed to Category II. The other Party shall then be notified immediately through the technical channel used in maintaining the joint lists, and shall similarly assign the crypto-system involved.

4. Category III shall contain:

- a. Crypt Intelligence except where specifically assigned to other Categories.
- b. Traffic Intelligence involving call-signs or message headings encrypted in codes or ciphers of high security grading.
- c. Traffic Intelligence involving such combination ("fusion") of separate Traffic Intelligence or other Category II sources as produces information whose value is so great that security of content becomes the overriding consideration.

d.

--

- e. Material involving sensitive collection procedures or the revelation of success against unusual, sensitive or complex transmission procedures and devices.

5. Sub-Categories shall be established as follows:

- a. Within Category II - None.
- b. Within Category III

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

- (1) Special Weather Intelligence /See NOTE 2b to Appendix B. This Sub-Category shall be designated by a separate codeword, and shall be considered less sensitive than the main body of Category III.

(2)



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

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~EO 3.3(h)(2)
PL 86-36/50 USC 3605APPENDIX BANNEXURE B2SECURITY PRINCIPLES GOVERNING THE CONDUCT OF COMINT ACTIVITIES INEXPOSED AREAS1. INTRODUCTION

It is recognized that effective interception of foreign communications and effective support of field commanders may require the establishment of COMINT activities in locations which may suddenly fall under unfriendly control with consequent loss of COMINT personnel and/or associated classified materials. It is agreed that, in addition to the pertinent, general provisions of Appendix B, the specific provisions which follow shall govern the conduct of COMINT activities in such locations.

2. DEFINITIONS

Exposed areas are those which are susceptible of being quickly overrun by enemy forces or those wherein the local political or military situation is such as to pose a distinct threat to the security of COMINT activities conducted therein.

[redacted] control and areas adjacent to these countries which are beyond defense lines expected to be tenable. In proportion to the risk of loss of COMINT personnel and/or classified material located therein, such areas involve three situations:

- a. Protected situations, i.e.: those in which there is no reasonable expectation of such a loss.
- b. Risky situations, i.e.: those in which it is likely that complete evacuation of COMINT personnel and removal or effective destruction of classified material will be accomplished.
- c. Dangerous situations, i.e.: those in which it is unlikely that complete evacuation of COMINT personnel and removal or effective destruction of classified material will be accomplished.

3. EVALUATION OF SITUATIONS IN EXPOSED AREAS

The decision whether a given situation is protected, risky or dangerous shall be made by USCIB or CRC, or by such other authorities as are responsible for the security of the COMINT activities concerned, and shall be made in the light of the political, military, and other factors affecting the safety of the COMINT personnel and materials involved.

4. FACTORS AFFECTING DECISIONS TO CONDUCT COMINT ACTIVITIES IN RISKY OR DANGEROUS SITUATIONS

COMINT activities shall be conducted in risky or dangerous situations only after due consideration of the COMINT losses which may result if the area concerned is suddenly attacked, and of the probable effect of such losses upon the conduct of COMINT activities elsewhere.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~5. SAFEGUARDS FOR RISKY SITUATIONS

In the case of COMINT activities established in risky situations, the following safeguards shall be applied save as exceptions to them are specifically approved by USCIB or CRC:

- a. Only intercept, analytic and reporting tasks which cannot be performed satisfactorily in safe or protected situations shall be assigned.
- b. No Category III COMINT or related documents and technical material shall be held except those essential to the assigned task and of current application thereto, and the latter shall be maintained in such condition as to insure immediate destruction, if necessary, upon sudden threat of seizure.
- c. No person in Group D, as defined in sup-paragraph 30d of Appendix B, shall be assigned, unless required by technical considerations.
- d. Facilities shall be provided with which one-third of the complement can be expected to destroy effectively, if necessary, all classified COMINT materials within a time limit commensurate with existing dangers, and unit personnel shall be skilled in the use of these facilities.
- e. Appropriate steps shall be taken to insure that adequate arrangements are made for safe evacuation of all personnel whose loss would be damaging and that the unit in question is kept informed of evacuation plans on a current basis.

6. SAFEGUARDS FOR DANGEROUS SITUATIONS

In the case of COMINT units established in dangerous situations the following safeguards shall be applied save as exceptions to them are specifically approved by USCIB or CRC:

- a. Only unique intercept tasks which cannot be accomplished elsewhere shall be assigned, and only such analysis as is locally required to support these tasks and permit essential technical reporting shall be performed.
- b. Only COMINT documents or technical aids essential and of current application to these tasks shall be held.
- c. No Category III COMINT or related documents and technical material shall be held.
- d. Personnel technically informed in COMINT of a higher level or broader scope than is required for the limited mission of the unit should not be assigned if avoidable.
- e. No person in Group C as defined in sub-paragraph 30c of Appendix B shall be assigned unless his presence is vital for the effective functioning of the unit.
- f. No person in Group D as defined in sub-paragraph 30d of Appendix B shall be assigned in any circumstances.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

- g. Facilities shall be provided with which the minimum number of persons on duty at any one time can be expected to destroy effectively, if necessary, all classified COMINT materials within a time limit commensurate with existing dangers, and unit personnel shall be skilled in the use of these facilities.
- h. Appropriate steps shall be taken to insure that the unit in question is kept informed of evacuation plans on a current basis.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~APPENDIX BANNEXURE B3MINIMUM STANDARDS FOR INVESTIGATIONAND CLEARANCE OF PERSONS TO BE INDOCTRINATED FOR COMINT ACTIVITIES

1. With reference to paras 22 and 23 of Appendix B, it is mutually agreed that the minimum standards for investigation and clearance of each person who handles or has access to COMINT material or information will be as follows:

- a. He shall be of excellent character and discretion, and of unquestioned loyalty. There shall be no exception to this requirement.
- b. He should be a citizen of the U.S., Canada or the UK and the members of his immediate family should also be citizens thereof.
- c. He should have no member of his immediate family or person to whom he may reasonably be supposed to be bound by ties of affection, kinship, or obligation, who is of dubious loyalty.
- d. He should have no member of his immediate family or person to whom he may reasonably be supposed to be bound by ties of affection, kinship, or obligation, who is a resident or a citizen of a foreign country having basic or critical national interests opposed to those of the U.S. and Canada.

Exceptions to any of the foregoing requirements except the first may be made only in a case of compelling need after every reasonable assurance has been obtained that, in the circumstances, the security risk involved is warranted.

2. To permit evaluation on the basis of the foregoing requirements, a thorough investigation shall be conducted as expeditiously as practicable, covering a sufficiently long period of the subject's life as to insure to the complete satisfaction of the clearing Agency that no reasonable doubt exists as to the security reliability of the subject.

3. Each person who is to be cleared for COMINT shall be thoroughly and carefully instructed in the doctrine and principles of COMINT protection, and in the regulations which govern the dissemination and safeguarding of COMINT, and shall be required to subscribe to an oath or declaration of secrecy.

4. When a person's "need to know" has ceased, he shall be debarred from further access to COMINT activities or results, and be required to subscribe to a final oath or declaration of secrecy.

5. Persons cleared for COMINT and retaining that status over a long period of time shall be the subject of such continuing investigative checks and security surveillance as investigative facilities permit.

~~TOP SECRET FROTH~~