

10 April 1952

REPORT BY THE USCIB SECURITY COMMITTEE

OF

MEASURES FOR THE INCREASED SECURITY

OF COMINT

THE PROBLEM

1. To consider what changes should be made in BRUSA COMINT regulations and practices in order to improve COMINT security and to increase the efficiency of the exploitation of COMINT sources.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Over the past year USCIB and its Security Committee have considered the need to make changes in present BRUSA COMINT regulations and practices in order to meet various problems affecting the security and dissemination of COMINT. Inter alia these problems have included:

- a. Certain substantial changes in the nature and products of BRUSA COMINT activities since BRUSA security regulations and practices were last regularized in 1948.
- b. The need to increase the utility of tactical military COMINT in Korea.
- c. The desirability of broadening the use of other low level COMINT material.
- d. The anticipated requirement to provide certain BRUSA COMINT products to third party recipients in NATO.
- e. The proposal to establish a NATO COMINT service.

- 1 -

~~TOP SECRET SURE - SECURITY INFORMATION~~

- f. Reporting relationships with third parties
- g. Planning for special BRSA collaboration in time of war
3. This report proposes certain specific changes to present BRSA CONTROL regulations and provisions which are designed to meet these problems. It is based on a detailed consideration of the following:
 - a. Reviews Security Committee reports on this subject (USCIB 13/163 dated 30 March 1951; USCIB 13/195 dated 21 July 1951; and USCIB 13/223 dated 14 January 1952)
 - b. Discussions in USCIB, particularly the terms of reference provided by the Chairman at the Sixty-seventh Meeting of the Board on 3 August 1951 (USCIB 13/190)
 - c. The final papers of the recent BRSA Conference in London (USCIB 14/206 dated 12 March 1952) which proposed new Appendices P and Q to the BRSA Agreement and a revision of the present Appendix O to the BRSA Agreement. These papers were approved by USCIB at its Seventy-fifth Meeting on 24 March 1952.
 - d. The "Proposed Definitions and Categories of CONTROL" which were prepared jointly and inferentially by the delegations to the recent BRSA Conference in London (USCIB 13/234 dated 18 March 1952). These proposals were approved in principle by USCIB at its Seventy-fifth Meeting on 24 March 1952.
 - e. Both the specific proposals which have been approved in principle by USCIB (13/234) and the other proposals submitted previously by the Security Committee will require certain changes in existing BRSA security regulations and provisions. The Security Committee has considered these changes in the light of the final papers of the recent BRSA Conference in London (14/206) and finds that they will involve substantial revisions of Appendix B to the BRSA Agreement. These revisions may be summarized as follows (references are to paragraphs in the draft of a new Appendix B which is enclosed herewith):
 - a. The removal of press and propaganda broadcasts from the body of Communication Intelligence as defined at present. (See para 3)

~~TOP SECRET SURE - SECURITY INFORMATION~~

~~TOP SECRET SUEBS - SECURITY INFORMATION~~

b. A change in the terminology applied to the categories of COMINT so as to:

- (1) Eliminate the term "Special Intelligence" and substitute therefor the term "Crypt Intelligence";
- (2) Discontinue use of the terms "Special Intelligence" ("Crypt Intelligence") and "Traffic Intelligence" as categories for the handling of COMINT and employ them as terms defining the sources of COMINT. (See paras 3b and 3c)
- (3) Establish new categories for the handling of COMINT. (See paras 3d and 3e)

c. The establishment of three categories for the handling of COMINT (Categories I, II and III) and provision for the subdivision of Categories I and II into various classes to permit differentiation in the handling and dissemination of materials within these categories. Allowance is made for the use of supplementary codewords for these additional, separate classes. Category III is reserved for certain low level COMINT materials to be handled on a non-codeword basis and disseminated to non-indoctrinated persons. (See paras 3f, 4-6, 10-11.)

d. The establishment of procedures for classification and codeword protection of these new handling categories as follows:

- (1) Category I to be TOP SECRET and to bear a TOP SECRET codeword. (See paras 8, 15, 31)
- (2) Category II to be SECRET and to bear a SECRET codeword. (See paras 9, 15, 31)
- (3) Category III to be classified not lower than CONFIDENTIAL and not to be designated by a codeword. (See para 10)

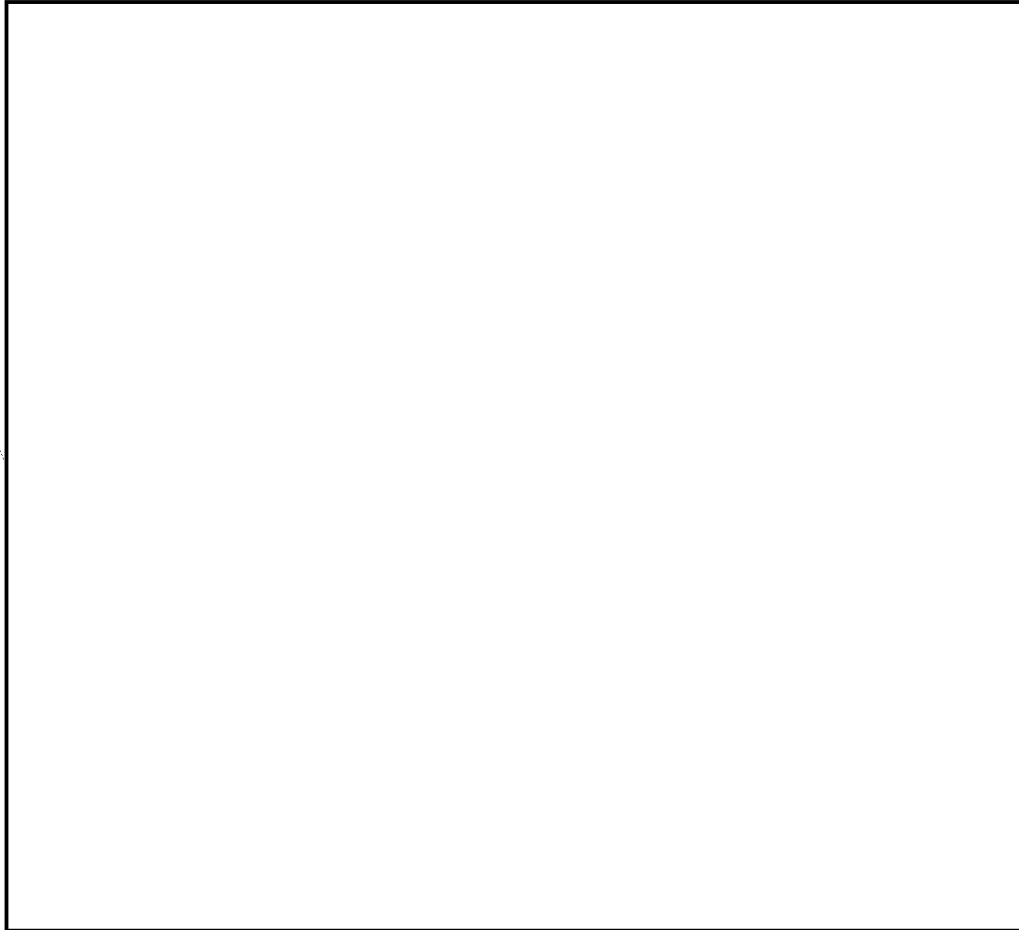
e. The establishment of a means whereby COMINT materials will be assigned to their appropriate categories; these assignments to be recorded and regularized through the establishment of an additional annexure to Appendix B. (See para 7)

~~TOP SECRET SUEBS - SECURITY INFORMATION~~

~~TOP SECRET SOURCE - SECURITY INFORMATION~~

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

f. The establishment of precise regulations for the dissemination of Categories I and II COMINT, including provision that:



g. The establishment of precise regulations for the dissemination of Category III COMINT, including provision that:

(1) Category III COMINT shall normally be handled via COMINT channels, but may be disseminated in the same manner as other intelligence materials of similar classification. (See paras 28 and 34)



- 4 -

~~TOP SECRET SOURCE - SECURITY INFORMATION~~

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

(3) Category III COMINT may not be disseminated by radio in plain language save in the form of operational orders when no suitable means of secure communications is available. (See para 26a)

h. The establishment of a clear definition of "suitable cover" for action to be taken on the basis of COMINT. (See para 27)

i. Provision for special handling and more limited dissemination of COMINT items requiring such treatment. (See para 29)

j. Elimination of the present arbitrary time limit governing the exposure of indoctrinated persons to hazardous conditions, and the substitution thereof of a provision requiring a determination in each instance based on the timeliness and sensitivity of the COMINT knowledge of the person whose assignment is in question. It is provided further that this determination shall be made only by senior officers or officials at a level to be established by USCIB and LSIB.

k. Provision that regulations governing standards for COMINT security investigations and clearance be exchanged between USCIB and LSIB. (See para 19)

l. Provision that USCIB and LSIB shall maintain lists of indoctrinated persons authorized to have access to both categories I and II COMINT. (See para 22)

m. Provision that USCIB and LSIB shall exchange lists of the total number of indoctrinated persons authorized to have access to both categories I and II COMINT. (See para 23)

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

~~TOP SECRET SUSEX - SECURITY INFORMATION~~

5. Upon revision of Appendix B and the assignment of COMINT materials to the appropriate new categories, it will be necessary to make appropriate corrections or revisions to the present annexure to Appendix B and to the other appendices to the BRUSA Agreement so that they will conform to the principles and terminology established in the new Appendix B.

CONCLUSIONS

6. Certain changes should be made now to BRUSA security regulations and practices in order to provide for the proposed definitions and categories of COMINT which have been approved in principle by USCIB and to meet other problems affecting COMINT security and dissemination which have been considered by USCIB and its Security Committee. These changes should include:

a. A substantial revision of Appendix B to include the changes listed in paras 4a-c above as presented in the draft of a new Appendix B which is attached as Inclosure 1.

b. The establishment of a new annexure to Appendix B which will list the detailed assignment of COMINT materials to the appropriate, new categories.

c. The correction or revision of the present annexure to Appendix B and the other appendices to the BRUSA Agreement so that they will conform to the principles and terminology of the new Appendix B.

RECOMMENDATIONS

7. It is recommended that:

a. The proposed new Appendix B (Inclosure 1) be approved by USCIB as a basis for negotiation with LSIB; a copy of this draft Appendix B to be forwarded to LSIB now.

b. The USCIB Coordinator be designated to have prepared:

(1) A proposed new annexure to Appendix B which will assign COMINT materials to the appropriate new categories

~~TOP SECRET SUSEX - SECURITY INFORMATION~~

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

(2) A list of resultant editorial corrections or revisions needed in the present annexure to Appendix B and the other appendices to the BRUSA Agreement.

c. Upon review and approval by USCIB of the draft annexure to Appendix B (b(1) above), the total documentation prepared by the USCIB Coordinator (b(1) and (2) above) be forwarded to LSIB.

d. USCIB designate a representative or representatives to negotiate with representatives of LSIB in revising Appendix B and making resultant changes in the other appendices to the BRUSA Agreement.

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~~~TOP SECRET - SECURITY INFORMATION~~DRAFT

10 April 1952

APPENDIX BTABLE OF CONTENTS

Para 1-4	Introduction	Page 2
<u>DEFINITIONS AND CATEGORIES</u>		
Para 3	Communications Intelligence, Crypt Intelligence and Traffic Intelligence	Page 2
Para 4	Category I COMINT	Page 3
Para 5	Category II COMINT	Page 3
Para 6	Category III COMINT	Page 4
Para 7	Precise Content of Categories	Page 4
<u>CLASSIFICATION AND CODEWORDS</u>		
Para 8	Category I COMINT	Page 4
Para 9	Category II COMINT	Page 5
Para 10	Category III COMINT	Page 5
Para 11	Classes of COMINT	Page 5
Para 12	Technical Material (Matter)	Page 5
Para 13	Documents	Page 5
Para 14	Raw Traffic	Page 5
Para 15	Codewords	Page 6

~~TOP SECRET - SECURITY INFORMATION~~~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~PRINCIPLES OF SECURITY

Para 16	Preservation of the Source	Page 6
Para 17	The Time Limit for Safeguarding COMINT	Page 6
Para 18	Protection of Indoctriated Persons	Page 7
Para 19	Security Investigations and Clearances	Page 7
Para 20	Indoctrination	Page 8
Para 21	Emergency Indoctrinations	Page 9
Para 22	Records of Indoctrinated Persons	Page 10
Para 23	Exchange of Records of Indoctrinated Persons	Page 10
Para 24	Access to COMINT Agencies	Page 10
Para 25	Custody of COMINT Materials	Page 10

PRINCIPLES OF DISSEMINATION

Para 26	The Need-to-Know	Page 11
Para 27	Dissemination of Categories I and II COMINT	Page 11
Para 28	Dissemination of Category III COMINT	Page 14
Para 29	Special Handling for Limited Distribution	Page 16
Para 30	Prohibition on Commercial Use	Page 16

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~PROCEDURES

Para 31	Application of Classifications and Codewords	Page 16
Para 32	Transmission of Category I COMINT	Page 17
Para 33	Transmission of Category II COMINT	Page 18
Para 34	Transmission of Category III COMINT	Page 18
Para 35	Transmission of Raw Traffic	Page 18
Para 36	Use of Special Cryptographic Channels or Ciphers	Page 18

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~APPENDIX BPRINCIPLES OF SECURITY AND DISSEMINATIONINTRODUCTION

1. These principles shall be the basis of all regulations for the security and dissemination of Communication Intelligence issued by or under the authority of USCIB or LSIB and other appropriate officials 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. To ensure uniform interpretation of what constitutes such accord, each party shall forward all such regulations to the other for information.

2. It is recognized that, while the following principles are in general of universal application, provision should be made for pertinent modifications in the event of war or emergency to ensure that the maximum operational benefit consistent with security is derived from the source. Provision is made hereunder for modification in specific situations. It is contemplated that in time of war, or exceptionally as agreed to jointly by USCIB and LSIB, additional regulations embodying emergency provisions shall be brought into force by the respective parties.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~EO 3.3(h)(2)
PL 86-36/50 USC 3605DEFINITIONS AND CATEGORIES

3. Communication Intelligence (COMINT) is the name given to all intelligence information and technical material (matter) resulting from the interception and study of telecommunications, except press and propaganda broadcasts, not originated by United States or British authorities.

a. The terms Communication Intelligence (COMINT) and Signal Intelligence (SIGINT) are synonymous.



c. Traffic Intelligence is that Communication Intelligence which results from traffic analysis (the study of procedure signals, callsigns, message headings, D/F bearings and other externals of communications) and from plain text, i.e., information produced by all means short of the actual cryptanalysis of the text of intercepted communications.

d. Communication Intelligence is divided into three categories, as follows:

- (1) Category I COMINT
- (2) Category II COMINT
- (3) Category III COMINT

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

e. Communication Intelligence will be placed in Categories I, II or III as mutually agreed by USCIB and LSIB from time to time.

f. As agreed by USCIB and LSIB, Categories I and II COMINT may be subdivided into separate classes in order to permit differentiation in the processing, exploitation, or dissemination of material requiring still more limited distribution.

4. Category I COMINT is that Communication Intelligence 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 Categories II and III

b. Crypt intelligence concerning weather derived from the communications of meteorological organizations.

c. Traffic intelligence involving callsigns or message headings encrypted in codes or ciphers of high security gradings as may be specified by USCIB and LSIB.

d. Other traffic intelligence and certain plain text material as specifically and mutually agreed by USCIB and LSIB.

5. Category II COMINT is that Communication Intelligence for which the protection of source or content is not always the overriding

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

consideration and for which a less rigid standard of security is considered an acceptable risk. In general it will include:

a. Crypt intelligence involving solution of codes, ciphers and special systems of low security grading as may be specified by USCIB and LSIB,

b. All plain text and traffic intelligence not specifically included in Categories I or III.

6. Category III COMINT is that Communication Intelligence which may be subject to the least stringent security regulations 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 agreed specifically and mutually by USCIB and LSIB.

7. USCIB and LSIB shall prepare and maintain in current status mutually agreed lists to indicate COMINT placed in Categories I, II and III and in such separate classes within Categories I and II as may be established. These lists shall be in the form of an annexure to this Appendix.

CLASSIFICATION AND CODEWORDS

8. Category I COMINT shall be classified TOP SECRET and shall be designated by a distinctive codeword agreed on from time to time by USCIB and LSIB, except that Crypt Intelligence concerning weather derived from the communications of meteorological organisations shall be designated by a separate codeword.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

9. Category II COMINT shall be classified SECRET and shall be designated by a distinctive codeword agreed on from time to time by USCIB and LSIB.

10. Category III COMINT shall be classified not lower than CONFIDENTIAL and shall not be designated by a codeword.

11. Classing. Whenever Categories I and II COMINT are subdivided into separate classes, each additional class shall be designated by a supplementary codeword agreed on from time to time by USCIB and LSIB.

12. Technical material (matter) appertaining to the production of COMINT shall bear the classification and codeword(s) appropriate to the most sensitive category and class of COMINT to which it relates. Such technical material (matter) shall be handled in accordance with the regulations applicable to that category and class.

13. Documents which reveal actual success, progress, or processes in the production of COMINT shall bear the classification and codeword(s) appropriate to the most sensitive category and class of COMINT to which they relate and shall be handled in accordance with the regulations applicable to that category and class, even though such documents may not reveal COMINT as such.

14. Raw traffic (i.e., intercepted traffic showing no evidence of processing for COMINT purposes other than the inclusion of a case number and/or an arbitrary traffic designator) shall be classified not lower than CONFIDENTIAL and shall not be designated by a codeword.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

15. ~~Code words~~ used to designate Categories I and II COMINT, and separate classes into which these categories may be subdivided, shall themselves be classified TOP SECRET and SECRET respectively, and their implications shall not be made known to non-indestrinated persons, nor shall these codewords be used in their codeword sense in the presence of non-indestrinated persons.

PRINCIPLES OF SECURITY

16. The value of Communication Intelligence in war and peace cannot be overestimated; conservation of the source 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 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. The provisions of these regulations shall apply to any intelligence which, in whole or in part, includes information which can be traced solely to COMINT sources.

17. The time limit for the safeguarding of COMINT as defined herein never expires. It is of the utmost importance that complete and absolute silence on all Communication Intelligence matters be maintained by those who have ever been contacted with Communication

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

Intelligence organizations and by all individual recipients of Communication Intelligence, whether past or present, unless and to the extent that they are freed from this obligation by unmistakable and categorical order of proper authority as shall be designated by the respective parties. If, at any time, indiscreet matter referring to Communication Intelligence 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, producers or recipients of Communication Intelligence from their continuous obligation to maintain silence in accordance with these regulations.

18. Every effort should be made to ensure that no persons who has knowledge of COMINT shall, as long as this knowledge is considered so timely and sensitive as to involve a substantial risk to the security of COMINT activities, if compromised, be assigned to or be engaged in activities which might reasonably be expected to place him in a position where he might be captured by an enemy or otherwise be forced to submit to questioning by third party nationals. Determination of the operation of this restriction shall be made in each instance only by senior officers or officials at a level to be established by USCIB and LSIB.

19. Except in categories of persons and in individual cases agreed upon from time to time by USCIB and LSIB, all persons to be assigned to Communication Intelligence duties or to become recipients

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

of Communication Intelligence shall be the subject of security investigations and clearances. To ensure that such investigations and clearances are similar in character, each party shall forward regulations governing them to the other for information. It is recognized that the standards for these investigations and clearances may differ depending upon the category of COMINT to which the individual in question will have access, and that such differences will be commensurate with the differences in the sensitivity of the COMINT materials involved.

20. All persons to be assigned to duties involving Categories I and II COMINT or to become recipients of these categories of COMINT 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). It will not be necessary to indoctrinate persons who will be recipients of Category III COMINT alone or whose duties will involve only this category of COMINT.

a. Knowledge of specific categories or classes of COMINT shall be made available to indoctrinated persons only 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 absolute minimum. It is recognized as consistent with this principle that there may be a substantial difference in the number of indoctrinated persons

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

having access to the different categories and classes of COMINT.

e. It shall be permissible for indoctrinated persons who have access to a less sensitive category or categories and class(es) 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 categories and class(es) 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 for which they have access.

21. In time of war or emergency, or under other specific conditions, as agreed by USCIB and LSIB, exceptional occasions may arise where it is considered essential for an individual to take up duties involving Communications Intelligence before a security investigation and clearance can be completed. In such cases, the person concerned may be suitably indoctrinated on the authority of such senior officers or officials as are 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.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

22. USCIB and ISIB shall maintain complete lists of persons currently having access to Categories I and II COMINT under their respective Governments.

23. USCIB and ISIB shall keep each other fully informed of the Departments, Ministries, Agencies, Offices, Headquarters, and Commands receiving Categories I and II COMINT, or either of them, or any one or more classes thereof, indicating the approximate number of indoctrinated persons having access to each category and class.

24. No national of one party shall be permitted access to the other party's COMINT agencies or COMINT materials or knowledge of the existence thereof, unless he has been approved by his parent agency or Board and has been properly indoctrinated. Such access or knowledge shall at all times be limited strictly to the category or categories and class(es) of COMINT for which the person concerned has been given access and approved by his parent agency or Board.

25. Except as implicitly involved in the operation of paragraphs 27 and 32 hereof, documents containing Categories I and II COMINT and technical material (matter) or information revealing actual success, progress or processes in the production of these categories of COMINT shall remain exclusively in the custody of indoctrinated persons, secure from examination by non-indoctrinated persons.

~~TOP SECRET - SECURITY INFORMATION~~

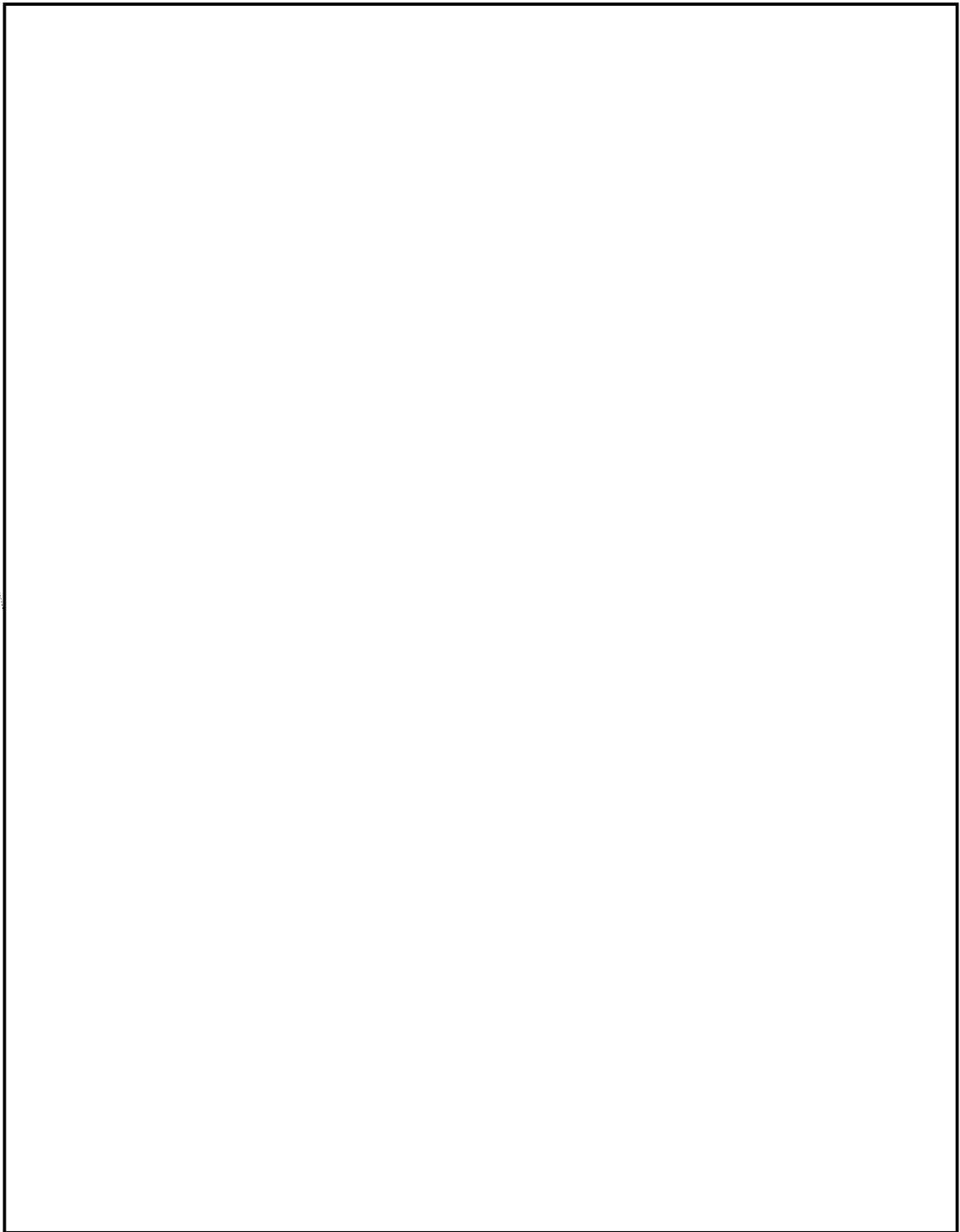
~~TOP SECRET - SECURITY INFORMATION~~EO 3.3(h)(2)
PL 86-36/50 USC 3605PRINCIPLES OF DISSEMINATION

26. The basic principle governing the production, exploitation, and dissemination 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 27 and 28 below, have been indoctrinated and authorized to have access to the particular category or class of COMINT to which such item appertains.

~~TOP SECRET - SECURITY INFORMATION~~

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

~~TOP SECRET - SECURITY INFORMATION~~

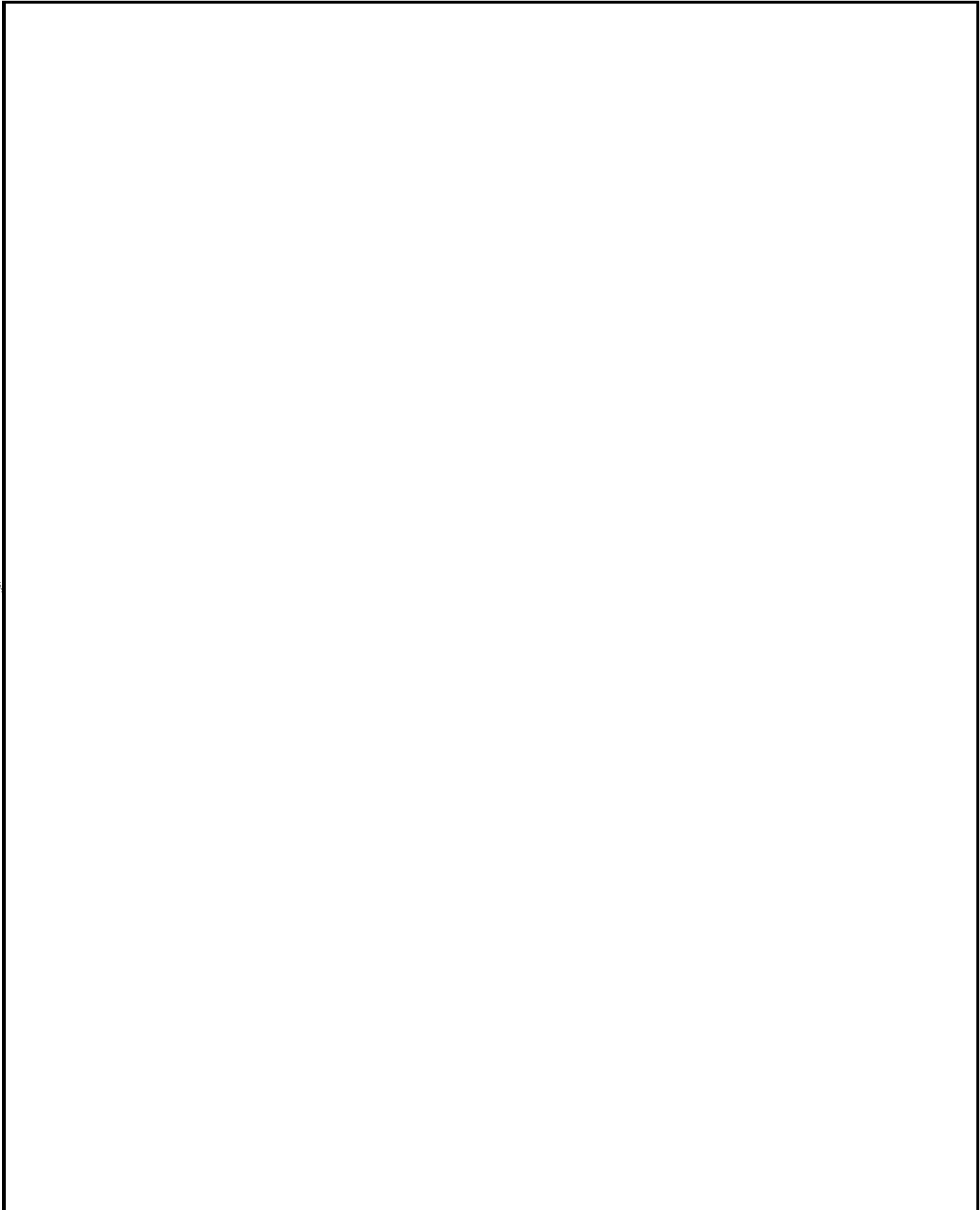


~~TOP SECRET - SECURITY INFORMATION~~

EO 3.3(h)(2)

PL 86-36/50 USC 3605

~~TOP SECRET - SECURITY INFORMATION~~



~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

g. In making the exceptions described in paragraphs 27g and g above, a studied effort shall be made to ensure that insofar as possible, action cannot be attributed to Categories I and II COMINT sources. Any necessary communication shall be so worded that the subject matter cannot be traced specifically to these sources (with names, times, positions, and other data identical with that from original decrypted texts omitted or carefully disguised wherever possible). If such a communication is to be transmitted by a means exposed to interception, it shall be encrypted in the available cryptographic channel or cipher of greatest security and most limited distribution. The COMINT enciphers shall not be used in connection with such a communication. Unindicated personnel involved are to be given only the minimum information they require.

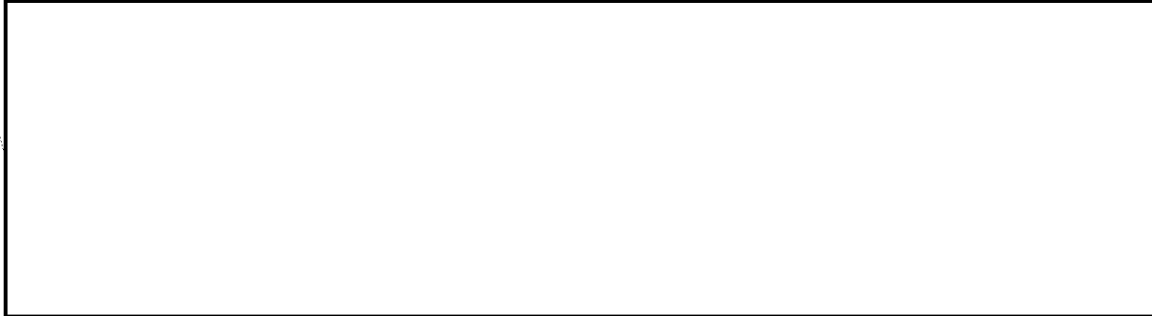
28. Category III COMINT may be disseminated in accordance with the normal practice of each party as regards intelligence materials of similar classification, provided that:

a. Whenever Category III COMINT, including any intelligence which in whole or in part can be traced solely to Category III COMINT sources, is to be transmitted by a means exposed to interception, it shall be transmitted in plain language only when there is no suitable means of secure communication. Such plain language transmissions shall be in the form of operational orders

~~TOP SECRET - SECURITY INFORMATION~~

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

so stated that the subject matter cannot be traced specifically to the COMINT sources.



c. Category III COMINT, including any intelligence which in whole or in part can be traced solely to Category III COMINT sources, shall not be disseminated to third party recipients except under the following conditions:

(1) In the event of COMINT arrangements with third parties within the framework of allied commands, Category III COMINT may be released to these third parties in accordance with the provisions of Appendix P and its pertinent annexures.

(2) During active military hostilities or in the case of an emergency involving a matter of importance to the national security of either party, Category III COMINT may be disseminated to nationals of third parties who are engaged directly with the US or UK in these hostilities or are allied directly with the US or UK in dealing with the emergency involved. The determination of a requirement to make this exception shall be made only by senior officers or officials at a level to be established by USCIB and LSIB.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

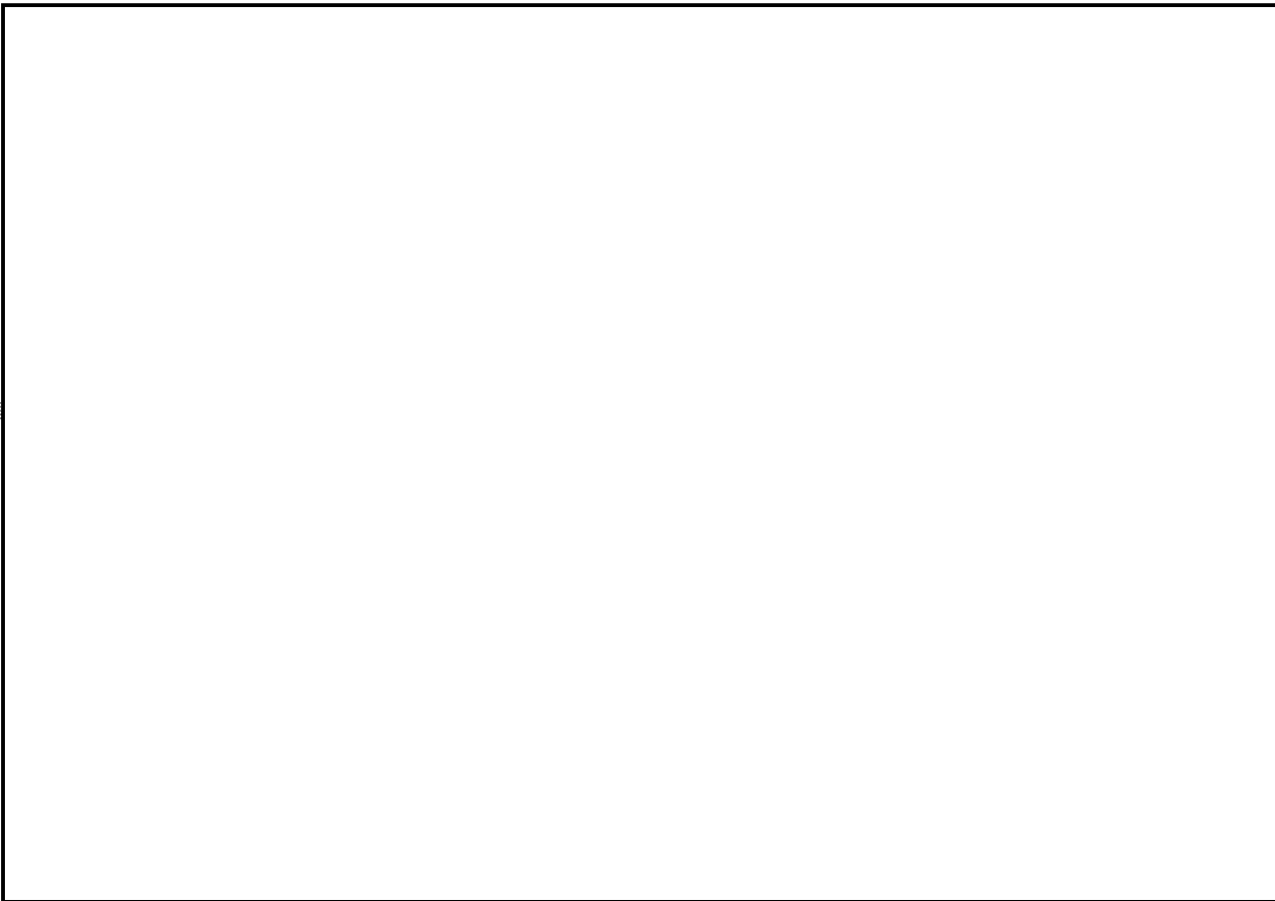
29. In the event that either party protects individual items of COMINT which, by reason of the extreme sensitivity of their source or content should be given a more limited dissemination than would normally be given to the category or class of COMINT within which they fall, it will be for the originating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

30. Communication Intelligence 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.

PROCEDURES

31. The appropriate classification and codeword shall appear on every sheet of paper which contains or discloses Categories I and II COMINT, technical material (matter) appertaining to these categories of COMINT, and documents which reveal actual success, progress or processes in the production of these categories of COMINT. This rule applies to maps and charts on which are plotted data and information derived from these categories of COMINT.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

32. Category I COMINT and TOP SECRET technical material (matter) shall not be transmitted in plain language except as follows:

a. Sealed, by safehand channels, over routes specifically approved by USCIB or ISIB. Such approval will be the exception where such routes involve air or land transport over the territory of a third party.

b. Over landlines specifically approved in each instance by USCIB or ISIB.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

e. Over completely protected local communications systems exclusively internal to agencies or offices producing or utilizing Communications Intelligence.

33. Category II COMINT and SECRET technical material (matter) shall not be transmitted in plain language except as provided in paragraph 32 above or by protected postal channels over routes approved by USCIB or LSIB.

34. Category III COMINT and CONFIDENTIAL technical material (matter) 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 paragraph 26g.

35. Raw traffic classified CONFIDENTIAL shall not be transmitted in plain language except as provided in paragraphs 32 and 33 above. The restrictions on the conveyance of raw traffic over the territory of third parties may be relaxed by USCIB or LSIB except that such relaxation will be the exception in the case of raw traffic originated by nationals of the third party involved.

36. Except as provided in paragraph 27g above:

a. Category I COMINT and TOP SECRET technical material (matter) transmitted in encrypted form shall be encrypted in special cryptographic channels or cyphers expressly provided for these subjects.

~~TOP SECRET - SECURITY INFORMATION~~

~~TOP SECRET - SECURITY INFORMATION~~

b. Category II COMINT and SECRET technical material (matter) transmitted in encrypted form shall be encrypted in special cryptographic channels or cyphers expressly provided for these subjects, those listed in paragraph a above, or in the highest grade cypher available.

c. However, in the case of COMINT or similarly secure cyphers, the transmission of Communication Intelligence, TOP SECRET and SECRET technical matters and raw traffic over the same channel is authorized, provided that such channels are reserved for these subjects exclusively.

~~TOP SECRET - SECURITY INFORMATION~~