GUIDE LINES FOR SECURITY CLASSIFICATION

8b

III II I

SECTION I - GENERAL

1. The classifying of information and material within the cryptologic field is an involved and complex problem. Every document to be classified must be considered as being unique and one whose classification is dependent on factors existing within that document alone. The decision as to the proper classification of a document cannot arbitrarily be determined by referral to other documents or to specific rules and regulations. Each item of information or material must be adjudged solely on its own merits and classified according to its content. There are, however, certain basic principles of classification which will be of assistance to individuals within the cryptologic field in the solution of their classification problems, and it is proposed to set forth these basic principles in this document.

2. As a basis for classification, it is necessary that all personnel be thoroughly conversant with the security classifications established by Executive Order 10501: TOP SECRET, SECRET and CONFIDENTIAL. These security classifications can be stated as follows:

a. Top Secret: Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only

6th rev. (Sect I 2-a cont)

to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

b. Secret: Except as may be expressly provided by statute, the use of the classification Secret shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

c. Confidential: Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

d. Confidential - Modified Handling Authorized: This does not constitute a separate and distinct classification category. Information must meet the requirements set down above for Confidential material. The addition of the notation "modified handling authorized" only permits modification of the storage and transmission procedures.

6th rev. (Section I cont)

3. Within the cryptologic field we must provide even more safeguards for our activities than are provided for under the standard security classifications. Before any official cryptologic information is to be disseminated, it must be determined that the recipient has a need-to-know. Information of an unclassified nature pertinent to the mission of cryptologic activity should not be discussed with anyone except for official business purposes.

4. Beyond the basic classifications established by Executive Order, we recognize that there are special considerations which must be recognized separately because of their inherently sensitive nature. These special considerations pertain to specific categories of communications intelligence (COMINT) and are identified by the assignment of a distinctive codeword. The classification of COMINT involves two distinct considerations: the security of the information and the sensitivity of the source from which the information was derived. Either or both considerations may affect the classification, dependent upon whether the information or the source is the more sensitive.

5. Initially, COMINT material comes to this Agency as raw traffic which has been intercepted by field station activities throughout the world. This traffic is classified no lower than CONFIDENTIAL until such time as an analytical processing is begun. From the analysis of this raw traffic, we derive three types of intelligence.

a. Cryptintelligence is that COMINT which results from cryptanalysis of the systems utilized by message originators to protect the traffic during its transmission. This includes speech and facsimile security systems.

b. Traffic intelligence is that COMINT which results from traffic analysis of intercepted electrical communications. This includes COMINT produced by all means short of cryptanalyses of message texts.

c. Intelligence derived from the analysis of plaintext traffic.

6. Information derived from these three analytical processes (cryptanalysis, traffic analysis and plaintext analysis) is divided into three security categories.

a. Category III COMINT (Top Secret Codeword) contains information of the highest classification and is the most sensitive category whose source must be protected at all costs. In general, this will include information derived from cryptanalysis (except for designated types of COMINT), special weather cryptanalysis and traffic analysis of certain high level systems as specified by existing authorities and highly informative plaintext.

b. Category II COMINT (Secret Codeword) is less sensitive than the preceding category in that protection of its source is not always the overriding consideration and is one which can, by acceptance of a calculated risk, be disseminated with a less rigid standard of security.

c. Category I COMINT (Non-Codeword) is subject to the least restrictive regulations of the three categories and will include certain types of low level COMINT as specified by existing authorities. Material in this category will be classified no lower than CONFIDENTIAL <u>without</u> the assignment of any codeword. Extreme care must be utilized in placing COMINT in this category. (See paragraph 7, Section VI - CONFIDENTIAL.)

7. In addition to these categories, there are certain other basic statements that are acceptable as guide lines in determining classifications.

6th rev. (Section I - 7 cont) ~~SECRET~~

a. COMINT will normally be considered as falling within Category III except for such specific systems as have been mutually agreed upon by UK and the U.S. to be in other categories. This list is available in PROD (NSA-0621).

b. Standing operating procedures, personnel reports, organizational charts and instructions manuals governing respective COMINT organizations will be classified according to the information contained therein; those indicating operational capacity or success will be classified at least SECRET. Classification problems which cannot be resolved by the originator will be referred to NSA Classification Advisory Panel.

c. In reference to type of cryptosystems, the terms "low grade", "medium grade" and "high grade" are often used. Definition of these categories are as follows:

(1) low-grade, Pertains to a cryptosystem which offers only slight resistance to cryptanalysis; for example: (1) Playfair ciphers, (2) Single transposition, (3) Unenciphered one-part codes.

(2) medium grade, Pertains to a cryptosystem which offers considerable resistance to cryptanalysis; for example: (1) Strip ciphers, (2) Polyphase transposition, (3) Unenciphered two-part codes.

(3) high-grade, Pertains to a cryptosystem which offers a maximum of resistance to cryptanalysis; for example: (1) Complex cipher machines, (2) one-time systems, (3) Unknown two-part codes enciphered with an additive book.

6th rev. (Section I cont)

~~SECRET~~

8. As a means of further assistance to personnel the following classification guide lines have been established. Remember they are only general in nature and that the classification of any given item must be established solely on its own merits. Utilization of these guide lines can only be done through analogy, comparison and evaluation. In any event the classification of a given item of information, such as training publications, will be SOLELY ON ITS OWN MERITS.

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

SECTION II - TOP SECRET CODEWORD [CATEGORY III]

The following types of information are to be classified TOP SECRET CODEWORD:

1. ~~Cryptanalytic intelligence produced from Category III systems.~~ All crypt intelligence produced from cryptosystems other than those listed for assignment in Category II or I.
2. ~~Traffic intelligence involving call-signs or message headings~~ encrypted in codes or ciphers of high security grading. ~~Exceptions would be listed separately.~~

3. Intelligence which can be identified as resulting from the study of

[redacted]

6. Traffic intelligence involving such combinations of cryptanalysis and traffic analysis whose value is so great that security of contents becomes the over-riding consideration.

7. COMINT based on [redacted] derived from sources classified TOP SECRET.

SECTION IV - TOP SECRET [CATEGORY I]

The following types of information are to be classified TOP SECRET:

1. The detailed mission of a COMINT agency or a major component thereof.

2. The existence of peacetime collaboration in COMINT matters between U. S. agencies and other foreign governments, except for collaboration with the U. K., Canada and Australia, which will be classified SECRET.

3. Intelligence derived from the cryptanalysis of high-grade foreign cryptosystems between 1 Sept 39 to 2 Sept 45, provided the reference cannot lead to inferences as to the specific systems involved. Such intelligence derived after 2 Sept qualifies in Category III. (See exceptions, paragraph 5, Section II - TOP SECRET CODEWORD and paragraph 12, Section VII - UNCLASSIFIED.)

SECTION III - SECRET CODEWORD [CATEGORY II]

The following types of information are to be classified SECRET CODEWORD:

1. Traffic intelligence derived from the analysis of foreign communications after 2 September 1945.

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

2. Texta information.

3. Intelligence which can be identified as resulting from study of

[redacted]

except as noted in paragraph 5, Section II - TOP SECRET CODEWORD.

4. Cryptanalytical intelligence produced from Category II cryptosystems.

SECTION V - SECRET

The following types of information are to be classified SECRET:

1. Intercept assignments.

2. Intercept and D/F plans and over-all operational effectiveness of intercept and D/F organization as a whole.

3. General reference to the fact of cryptanalytic success against low-grade enemy military cryptosystems during World War II and the Korean conflict, without any detailed description of the cryptanalytic methods used.

4. Details of traffic analysis as applied to enemy communications during World War II.

5. Description of COMINT equipment peculiar only to intercept stations.

6. Detailed listing and location of US Service operated COMINT intercept stations.

7. Existence of peacetime collaboration between the US (NSA), UK (GCHQ), Canada (CBNRC), and Australia (DSB) in the COMINT field.

8. Codewords (current and obsolete) applicable to Category II COMINT.

9. Information relating to an entire system of cryptologic (R/D) equipment.

10. Cryptanalytic short titles.

11. Disclosures of both the identity and details of the cryptanalysis of low-grade enemy military cryptosystems during World War II.

SECTION VI - CONFIDENTIAL

The following types of information are to be classified CONFIDENTIAL:

1. Association of operational COMINT functions with specific activities and organizations by name (except as provided under paragraph 1, Section VII - UNCLASSIFIED).

2. General statements pertaining to the operational effectiveness of individual intercept and D/F stations.

3. Intercepted raw traffic that shows no evidence of "processing" for COMINT purposes. Processing does not include case notations, frequencies, or call signs.

4. 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 complex changing callsign systems are included.

5. The terms "United States Communication Intelligence Board" and "U. S. Communication Security Board" (abbreviations "USCIB" and "USCSB" and the abbreviations for their subcommittees are unclassified).

6. Plaintext tactical or operational traffic provided that no interpretations of complex changing callsign systems, enciphered map references, or results or 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.

7. Intelligence derived 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 callsign 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.

8. COMINT concerning weather derived from the sources described in paragraphs 6 and 7, above.

9. Special Intelligence from Naval tactical maneuvering codes and brevity codes.

10. Special cryptologic features of and magnitude of effort with computers.

11. Detailed references to, and description of, cryptanalytic success against specific military cryptosystems used by foreign powers between 11 November 1918 and 1 September 1939, and not used since.

12. Intelligence derived from the cryptanalysis of the [redacted] between 11 November 1918 and 1 September 1939.

13. The extent of collaboration in CAN/UK/US COMSEC matters.

14. The extent of production of cryptomateriel for NATO use.

15. The fact that NSA is assigned specific [redacted]

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

16. Diagrams and descriptions of COMINT and COMSEC communication networks or related communication plans including cryptographic arrangements except where higher classification is justified by the listing of sensitive intercept stations.

17. Consolidated listings and records of cryptomaterials and crypto-holdings by short title.

18. The broad outlines of Operational Traffic analysis processes.

19. Relationship with CIA and other consumers in the field of COMINT.

SECTION VII - UNCLASSIFIED

The following types of information are Unclassified:

1. Association of NSA with cryptology, COMINT or COMSEC and the service cryptologic agencies --- providing such association in no way adversely affects the missions of the agencies concerned.

2. Association of NSA with authors of technical papers on matters already in the public domain.

3. The terms NSA Field Activity Far East (NSAFE), NSA Field Activity Europe (NSAEUR), NSAAL, NSAUK, NSA-Field Unit 1 (FU/PAC) and NSA Field Unit 2 (FU/LANT).

4. Civil Service Job Titles and NSA "Qualification Standards Manual".

5. NSA's possession of or interest in computers or rapid analytical machinery, except as noted in Paragraph 10 under Section VI - CONFIDENTIAL.

6. Specific components of equipment under research, if use of component is not revealed.

7. Report of inspection trip to uncleared company that is a prospective contractor, if no mention is made of actual applications of components.

8. Short titles, cover names, and code words. (See the following exceptions: Paragraph 4, Section III - TOP SECRET: paragraph 9, Section V - SECRET; paragraph 10 Section V - SECRET, and paragraph 17, Section VI - CONFIDENTIAL.

9. Communications giving a person's security clearance and type of indoctrination.

10. Projects number and titles used in justification for purchase of materials when no technical usage is specified.

11. Detailed reference to, and description of, cryptanalytic success against World War I military cryptosystems.

12. References to intelligence derived from cryptosystems in which successful cryptanalysis has already been revealed by official U. S. action (e.g., the Congressional investigation of the Pearl Harbor attack).

13. Any reference to intelligence or cryptanalytic success against operational cryptosystems as disclosed by foreign publications appearing in the public domain. These references should be accompanied for the purpose of clarity by the source and be without further elaboration or amplification.

14. The fact that NSA produces and procures cryptomaterial including rotors, key lists, one-time tapes, one-time pads, codes, discs and other broad categories of keying materials, and employs special equipment to produce some of this material.

15. The fact that the US collaborates with other NATO powers on COMSEC matters.

CATEGORIES OF COMINT
UNDER CONSIDERATION BY USCIB

I. CATEGORY I

A. Assigned -

[redacted]

3. D/F mission assignments, bearing reports and fix reports as set forth in subparagraph 2a, Annexure B1, Revised Appendix "B", UKUSA Agreement.

B. Suitable for Assignment to Category I -

Other plaintext, traffic intelligence or crypt intelligence as set forth in paragraph 2, Annexure B1, Revised Appendix "B".

II. CATEGORY II

A. Assigned -

1. All traffic intelligence including plain text except that specifically assigned to Categories I or III herein.

2. Crypt intelligence produced from the cryptosystems listed in the attached Annex 1.

3. Freely available privacy and brevity systems such as commercial codes.

4. Traffic intelligence derived from [redacted] and TINA.

B. Suitable for assignment to Category II -

Crypt intelligence produced from the cryptosystems listed in the attached Annex 2.

III. CATEGORY III

A. All crypt intelligence produced from cryptosystems other than those listed for assignment to Category II or category I above.

B. Traffic intelligence based in whole or in part on the analysis or use of identifications and other data derived from Category III COMINT.

C. COMINT based on traffic obtained from sources, ~~the existence of which is~~ classified TOP SECRET.

EO 3.3(h)(2)
(b)(3)-50 USC 3507

D. Sub-categories of Category III:

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]