~~SECRET~~ 5th Revision: 1 June 54

GUIDE LINES FOR SECURITY CLASSIFICATION

See USCIB 14.1/

SECTION I - GENERAL

1. The classifying of information and material within the National Security Agency 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 reference to other documents or to specific rules and regulations. Each item of information or material must be adjudged solely on its own merits and shall be classified according to its own content. There are, however, certain basic principles of classification which will be of assistance to individuals within NSA in the solution of their classification problems, and it is proposed to consider 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 the Department of Defense: TOP SECRET, SECRET and CONFIDENTIAL (it will be noted as of 15 December 1953 the classification category RESTRICTED

was abolished by Executive Order No. 10501). By definition 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 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,

SECRET 5th Revision, 1 June 51

by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

3. Within the National Security Agency we must provide even more safeguards to our activities than are provided for under the standard security classifications. Before any official agency information is to be disseminated it must be determined that the recipient has a need-to-know. All information of an unclassified category, pertinent to the mission of NSA activities generally, should not be discussed with anyone except for official business purposes.

4. Beyond the basic classifications established by the Department of Defense, we recognize that within the National Security Agency, there are special considerations which must be recognized separately due to special considerations their inherently sensitive nature. These are the classifications pertaining to specific categories of communications intelligence information and which are identified by the assignment of a distinctive code word.

→ Define COMINT

5. The classification of COMINT involves two distinct considerations: the security of the information contained within an individual document and the sensitivity of the source from which this information was derived. Either or both considerations may affect the classification, dependent upon whether the information or the source is the more sensitive. 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 CONFIDENTIAL until such time as any analytical processing is begun.

~~UKUSA~~ 5th Revision: 1 June [illegible]

From the analytic processing of this raw traffic, we derive three types of information:

a. Cryptointelligence which results from successful analysis and solution of the cryptosystems which were utilized by the originators to protect the traffic during its transmission.

b. Traffic intelligence which results from the analysis of the external characteristics of the enciphered or encoded message. ↩ in accordance with UKUSA

c. Information that is derived from analysis of plaintext traffic.

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

a. Category III ~~COMINT~~ is of the highest classification and most sensitive category and is applied to that material whose source must be protected at all costs. In general, this data includes information derived from cryptanalysis ~~intelligence~~ analysis (except for certain specifically exempt categories), [redacted] cryptanalysis, ~~intelligence~~ analysis and traffic ~~intelligence~~ analysis of certain high level systems ~~which have been predetermined by existing directives to fall within this category.~~ as specified by existing authorities. It is this material in Category III which is considered to be TOP SECRET Codeword. (See Section II)

b. Category II ~~COMINT~~ is less sensitive than the preceding category and is one whose material can by acceptance of a calculated risk be disseminated without over-riding concern for the security of ~~it~~ the material in that protection of its source is not always the overriding consideration with a less rigid standard of security

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

~~SECRET~~ 5th Revision: 1 June 54

~~the source~~. This category will include traffic intelligence which has not been specifically placed into other categories and crypt intelligence resulting from the solution of certain low level codes and other security systems. It is this material in Category II which is considered to be TOUCH Codeword. (See Section IV)

c. Category I COMINT is subject to the least restrictive of the limitations of the three categories and will include certain types of low level COMINT ~~that will be predetermined by existing directives~~ as specified by existing authorities. Material in this category will be classified CONFIDENTIAL without the use of any codeword. Extreme care must always 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.

a. COMINT will normally be considered as falling within Category III except for such specific systems as have been mutually agreed upon by ~~USCIB~~ UK and the U.S. to be ~~down-graded to Category II~~ 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.

c. The problem of classifying organizational charts because of variable aspects involved is considered to be sufficiently sensitive to merit ~~Category~~ Security Classification

Panel. Charts which are proposed for publication will be sent to the AG for reference to this Panel as required.

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

(1) low-grade, adj. Pertaining 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, adj. Pertaining 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, adj. Pertaining 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.

8. As a means of further assistance to personnel within NSA the following classification guide lines have been established. Remember, however, they are only general in nature and cannot be applied to specifically each classification problem. 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.

~~SECRET~~

5th Revision: - June 54

SECTION II - TOP SECRET CODEWORD

a. Traffic Intelligence involving call-signs or message headings encrypted in codes or ciphers of high security grading. Exceptions would be listed separately.

2. Intelligence derived from the study of plaintext which is passed

[redacted]

paragraph 3, Section III - TOP SECRET, paragraph 12, Section VI - CONFIDENTIAL, and paragraph 12, Section VII - UNCLASSIFIED.

SECTION III - 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 U.K. collaboration which is SECRET.

3. Intelligence derived from the cryptanalysis of high-grade foreign cryptosystems during World War II, provided the reference cannot lead to inferences as to the specific systems involved. (See exceptions, paragraph 5, Section II - TOP SECRET CODEWORD, and paragraph 12, Section VII - UNCLASSIFIED.)

~~SECRET~~ 5th Revision: 1 June 54

4. Codewords applicable to Category III COMINT (current & obsolete)

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

6. Material involving sensitive collection procedures or the revelation of success against unusual or sensitive transmission procedures and devices.

NO

SECTION IV - SECRET CODEWORD

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

2. Texta information.

3. Intelligence ~~derived~~ which can be identified as resulting from study of [redacted], except as noted in paragraph 4, Section II - TOP SECRET CODEWORD, and paragraph 6, Section III - TOP SECRET.

4. MOA & REP
5. Brevity Codes

SECTION V - SECRET

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

1. Intercept assignments.

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

IP12

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.

~~TOP SECRET~~ 5th Revision: 1 June 54

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

7. Existence of peacetime collaboration between the US and UK (~~CANADA~~) in the COMINT field.

8. All personnel reports for the entire Agency, civilian or military, which indicate authorized or actual strength by organizational element, short title or symbol, or by function.

9. Codeword applicable to Traffic Intelligence.

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

11. Cryptanalytic short titles.

SECTION VI - CONFIDENTIAL

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

2. Individual intercept and D/F station products and statements of operational effectiveness.

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" 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.

~~SECRET~~ 5th Revision: 1 June 54

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

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

14. The extent of production of cryptomaterial [redacted]

15. The fact that NSA is assigned [redacted]

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 cryptoholdings by short title.

18. The broad outlines of Operational Traffic Analysis processes.

SECTION VII - UNCLASSIFIED

1. Association of NSA with cryptology; non-specific or hypothetical references to Communication Intelligence or Communication Security without any association of that function with specific activities and organizations other than the National Security Agency as a whole and Service cryptologic agencies as a whole; and association of NSA with the ~~latter~~ Service cryptologic agencies as a whole

2. Identification with NSA of NSA 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-FWPU (LANT), and NSA-FWPU (PAC).

4. Civil Service Job Titles and NSA "Classification 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 II - TOP SECRET CODEWORD; paragraph 4, Section III - TOP SECRET; paragraph 9, Section V - SECRET; paragraph 11, 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.