~~SECRET~~

Miscellaneous: Memos
Regs. etc.

Mr. William F. Friedman
310 Second St, S.E.
Washington, D.C

6

~~SECRET~~

Record taken from
WFF's home

Mr William F Friedman
310 Second St S.E.
OFFICIAL COURIER

SECRET

~~SECRET~~

APPENDIX

GUIDE LINES FOR SECURITY CLASSIFICATION

AG Pub

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 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.

See Section VII
Supersedes
+ Talk to R+L

Appendix to NSA Regulation
Number 121-7 dated 8 April 1955

~~HANDLE VIA COMINT~~
~~CHANNELS ONLY~~

SECRET

~~SECRET~~

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.

e. "For Official Use Only". This is not a security classification but is a designation to be used to assure the proper custody, preservation and use of official information which requires protection in public interest, but is not within the purview of Executive Order No. 10501.

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 a cryptologic activity should not be discussed with anyone except for official business purposes.

4. Beyond the basic classifications established by Executive Order, it is recognized that there are special considerations which must be considered 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 in the form of collateral COMINT or as raw traffic which has been intercepted by field

~~SECRET~~

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 cryptanalysis 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) is the most sensitive category and contains information of the highest classification whose source must be protected at all costs. In general, this will include information derived from cryptanalysis (except for designated types of COMINT) certain designated types of plaintext and special weather cryptanalysis and traffic analysis of certain high level systems as specified by existing authorities. For additional items in this category, 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 the source. In general, this will include traffic intelligence resulting from the solution of certain low level codes and other security systems as specified by existing authorities. For additional items in this Category, see Section III.

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 without the assignment of any codeword. Extreme care must be utilized in placing COMINT in this category. (See paragraph g, 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 [redacted] and the U. S to be in other categories. This list is available in PROD (0621).

b. Standing operating procedures, personnel reports, organizational charts and instruction 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 the Adjutant General for determination.

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

(1) Low-grade, Pertains to a cryptosystem which offers 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

8. It must be pointed out that, although the cryptanalytic techniques associated with a specific operational cryptosystem fall into Categories III, II, or I, nevertheless a detailed description of the procedures and general principles underlying the solution of a type cryptosystem may be of lower classification or even unclassified, e.g., the solution of the classic Playfair system. This consideration applies also to principles and techniques involved in the attack on U.S. [redacted] cryptosystems.

a. Likewise, although it must be pointed out that traffic analytic techniques and data associated with specific targets fall into Categories III, II or I, nevertheless a detailed description of the general principles and techniques involved in hypothetical traffic analysis may be of lower classification.

b. The classification of an item of cryptanalytic or cryptographic equipment is determined solely on its own merits, based on the extent to which protection of new principles and techniques must be afforded. The

degree of classification does not necessarily concern only the field of cryptology (or cryptologic aspects) but also takes into account engineering sophistication.

9. 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. In addition, an abbreviated classification table has been inclosed at the end of this document and is intended for reference purposes only. It may be detached and used separately. WARNING! In no instance may this table be used to solve classification problems. Reference must always be made to the complete text of "Guide Lines for Security Classification".

SECTION II - TOP SECRET CODEWORD (CATEGORY III)

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

a. Cryptanalytic intelligence and techniques derived from any statements of success attributable to a given Category III system.

b. Traffic intelligence based in whole or in part on the analysis or use of identifications and other data derived from Category III COMINT. Such traffic intelligence might involve a highgrade encryption system or message headings encrypted in codes or ciphers of high security grading.

c. Intelligence which can be identified as resulting from the study of plain text which is passed on [redacted] circuits and is of such high intelligence value of sensitivity as to require assignment to this category. PL 86-36/50 USC EO 3.3(h)(2)

d. Special Weather Intelligence, which does not contain information concerning the processes or sources involved will be designated by a distinctive codeword.

e. Intelligence which can be identified as resulting from the cryptanalysis of diplomatic cryptosystems used by foreign powers since 1 September 1939, except as covered in sub-paragraph c, Section IV - TOP SECRET; sub-paragraph 1, Section VI - CONFIDENTIAL; and, sub-paragraph 1, Section VII - UNCLASSIFIED.

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

~~SECRET~~

g. COMINT based on traffic obtained from sources classified TOP SECRET.

h. [redacted] Cryptanalytic short titles of Category III cryptosystems. PL 86-36/50 USC EO 3.3(h)(2)

SECTION III - SECRET CODEWORD (CATEGORY II)

The following types of information are to be classified SECRET Codeword.

a. Cryptanalytic intelligence and techniques derived from and statements of success attributable to a given Category II cryptosystem.

b Traffic intelligence derived from the analysis of foreign communications after 2 September 1945 except as covered in sub-paragraph b, Section II above.

c. Texta information. PL 86-36/50 USC 3605 EO 3.3(h)(2)

d. Intelligence which can be identified as resulting from study of Government, commercial or private plain text passed on [redacted] circuits, except as noted in sub-paragraph e, Section II - TOP SECRET Codeword.

e. Traffic intelligence derived from radio fingerprinting (RFP) and Morse operator analysis (MOA).

f. [redacted] Cryptanalytic short titles of Category II and I cryptosystems

SECTION IV - TOP SECRET

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

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

b. The existence of peace time collaboration in COMINT matters between U S. agencies and other foreign governments, except for collaboration with the U.K., Canada, or Australia, which will be classified not lower than SECRET.

c. Intelligence derived from the cryptanalysis of high-grade foreign cryptosystems between 1 September 1939 and 2 September 1945, provided the reference cannot lead to inferences as to the specific systems involved. Such intelligence derived after 2 September 1945 belongs in Category III. (See exceptions, sub-paragraph e, Section II - TOP SECRET CODEWORD and paragraph 1, Section VII - UNCLASSIFIED.)

d. Codewords (current and obsolete) applicable to Category III COMINT.

SECTION V - SECRET

The following types of information are to be classified SECRET:

a. Intercept assignments (N.B. This does not include call signs, frequencies or case notations which will be classified not lower than CONFIDENTIAL).

b. Intercept and DF plans and over-all operational effectiveness of intercept and DF organizations as a whole.

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

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

e. Existence of peace time collaboration between the U. S. (NSA) with the U.K. (GCHQ), CANADA (CBNRC) or AUSTRALIA (DSB) in the COMINT field.

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

SECTION VI - CONFIDENTIAL

The following types of information are to be classified CONFIDENTIAL:

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

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

c. Intercepted raw traffic that shows no evidence of "processing" for COMINT purposes beyond sorting by clear address elements, elimination of unwanted messages and the inclusion of case number and/or an arbitrary traffic designator.

d. Information about 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 complex changing call sign systems are included.

~~SECRET~~

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

f. 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.

g. 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 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.

h. COMINT concerning weather derived from the sources described in paragraphs f and g, above.

i. COMINT derived from Naval tactical maneuvering codes and brevity codes.

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

k. 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.

l. Intelligence derived from the cryptanalysis of the diplomatic cryptosystems used by foreign powers between 11 November 1918 and 1 September 1939.

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

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

n. The extent of production of cryptomaterial [redacted] use.

[redacted]

p. 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.

~~HANDLE VIA COMINT CHANNELS ONLY~~

q. Consolidated listings and records of cryptomaterials and cryptoholdings by short title.

r. The broad outlines of operational traffic analysis processes.

s. Relationship with CIA and other U.S. consumers in the field of COMINT.

SECTION VII - UNCLASSIFIED

The following types of information are UNCLASSIFIED:

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

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

c. 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).

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

e. NSA's possession of or interest in computers or rapid analytical machinery, except as noted in sub-paragraph j under Section VI - CONFIDENTIAL.

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

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

h. Short titles, cover names, and code words. (See the following exceptions: Sub-paragraph d, Section IV - TOP SECRET; Sub-paragraph f, Section V - SECRET and sub-paragraph q, Section VI - CONFIDENTIAL).

i. Communications giving a person's security clearance.

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

k. Detailed reference to, and description of, crypt-analytic success against World War I military cryptosystems.

l. 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).

m. 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.

n. 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.

o. The fact that the U.S. collaborates with other NATO powers on COMSEC matters.

SECTION VIII - FOR OFFICIAL USE ONLY

The following types of information, when unclassified, are to be designated "For Official Use Only":

a. Textbooks, syllabi, language dictionaries, telephone directories, etc., which of themselves do not warrant classification, however the wide dissemination of which might be detrimental to the security of the Agency's mission.

b. Records and information which pertain to individuals such as personnel records, medical records, and investigative reports, documents, and proceedings.

c. Information as to the identity of confidential informants and information furnished by them in confidence.

d. Information received in confidence from private individuals, firms, or organizations in connection with bids, proposals, "trade secrets", and reports of a financial, technical, or scientific nature.

e. Information which is, or may reasonably be expected to be, connected with any pending or anticipated litigation before Federal and state courts or regulatory bodies.

f. Advance information on proposed plans to procure, lease or otherwise acquire or dispose of materials, real estate, facilities, or functions, which would provide undue or discriminatory advantage to private or personal interests.

g. Preliminary documents relating to proposed plans and policy development when premature disclosure would adversely affect morale, efficiency or discipline.

h. Examination questions and answers to be used in training courses or in the determination of qualifications of candidates for employment, entrance to duty and advancement or promotion.

Incl:
Table

SECURITY CLASSIFICATION REFERENCE TABLE

(Warning! In no instance may this table be used to solve classification problems. Reference must always be made to the complete text of "Guide Lines for Security Classification.")

SECRET

TOP SECRET CODEWORD

1. INTELLIGENCE TECHNIQUES AND SUCCESSES ATTRIBUTABLE TO CATEGORY III SYSTEMS
2. TRAFFIC INTELLIGENCE BASED ON DATA DERIVED FROM CATEGORY III COMINT
3. [redacted]
4. SPECIAL WEATHER INTELLIGENCE (SPECIAL CODEWORD)
5. CRYPTANALYSIS OF DIPLOMATIC SYSTEMS, USED SINCE 1 SEPTEMBER 1939, EXCEPT[1].
6. TRAFFIC INTELLIGENCE WHERE SECURITY OF COMINT IS THE DOMINANT CONSIDERATION
7. COMINT BASED ON TOP SECRET SOURCES
8. [redacted] CRYPTANALYTIC SHORT TITLES OF CATEGORY III SYSTEMS

SECRET CODEWORD

1. INTELLIGENCE TECHNIQUES AND SUCCESSES ATTRIBUTABLE TO CATEGORY II SYSTEMS
2. TRAFFIC INTELLIGENCE DERIVED FROM FOREIGN COMMUNICATIONS AFTER 2 SEPTEMBER 1945.
3. TEXTA INFORMATION.
4. [redacted] PLAINTEXT, EXCEPT[1].
5. TRAFFIC INTELLIGENCE DERIVED FROM REP AND MOA
6. [redacted] CRYPTANALYTIC SHORT TITLES OF CATEGORY II AND I SYSTEMS

CONFIDENTIAL

1. COMINT FUNCTIONS ASSOCIATED WITH SPECIFIC ACTIVITIES AND ORGANIZATIONS BY NAME, EXCEPT[1].
2. GENERAL STATEMENTS OF OPERATIONAL EFFECTIVENESS OF INDIVIDUAL INTERCEPT AND D/F STATIONS.
3. UNPROCESSED RAW TRAFFIC EXCEPT CASE NOTATIONS, FREQUENCIES, OR CALL SIGNS
4. D/F MISSION ASSIGNMENTS
5. USCIB AND USCSB WHEN WRITTEN OUT
6. PLAINTEXT EXCEPT AS ASSIGNED TO CATEGORY II AND III.
7. UNENCIPHERED RADAR TRACKING AND VISUAL OPERATIONAL REPORTS.
8. WEATHER COMINT FROM 6 AND 7 ABOVE
9. COMINT FROM NAVAL MANEUVERING AND BREVITY CODES
10. FEATURES AND EXTENT OF USE OF COMPUTERS
11. CRYPTANALYSIS OF MILITARY SYSTEMS, 11 NOVEMBER 1918 - 1 SEPTEMBER 1939 AND NOT USED SINCE
12. CRYPTANALYSIS OF DIPLOMATIC SYSTEMS, 11 NOVEMBER 1918 - 1 SEPTEMBER 1939
13. CAN/UK/US COMSEC COLLABORATION
14. [redacted]
15. [redacted]
16. COMINT AND COMSEC COMMUNICATIONS NETWORKS OR PLANS EXCEPT FOR SENSITIVE INTERCEPT STATIONS.
17. CONSOLIDATED LISTINGS OF CRYPTO MATERIALS AND CRYPTO HOLDINGS BY SHORT TITLE.
18. BROAD OUTLINES OF OPERATIONAL TRAFFIC ANALYSIS PROCESSES.
19. COMINT RELATIONSHIP OF NSA WITH CIA AND OTHER US CONSUMERS IN THE FIELD.

UNCLASSIFIED

1. NON-SPECIFIC ASSOCIATION OF NSA WITH CRYPTOLOGY, COMINT, COMSEC OR SERVICE CRYPTOLOGIC AGENCIES.
2. ASSOCIATION OF NSA WITH AUTHORS OF TECHNICAL PAPERS ALREADY IN THE PUBLIC DOMAIN
3. NAMES OF NSA FIELD UNITS
4. CIVIL SERVICE JOB TITLES AND NSA "QUALIFICATION STANDARDS MANUAL."
5. NSA POSSESSION OF OR INTEREST IN COMPUTERS, EXCEPT[1].
6. NON-DESCRIPTIVE REFERENCES TO EQUIPMENT UNDER RESEARCH.
7. REPORTS OF INSPECTION TRIPS TO UNCLEARED PROSPECTIVE CONTRACTOR COMPANIES.
8. SHORT TITLES, COVER NAMES, AND CODEWORDS, EXCEPT[1].
9. COMMUNICATIONS GIVING A PERSONS SECURITY CLEARANCE
10. NON-DESCRIPTIVE USE OF PROJECT TITLES AND NUMBER.
11. CRYPTANALYTIC SUCCESS AGAINST WORLD WAR I MILITARY CRYPTOSYSTEMS.
12. CRYPT SUCCESSES IN THE PUBLIC DOMAIN
13. [illegible]
14. NSA PRODUCTION AND PROCUREMENT OF CRYPTO MATERIAL.
15. US COMSEC COLLABORATION WITH NATO

SECRET

TOP SECRET

1. DETAILED MISSION OF A COMINT AGENCY OR MAJOR COMPONENT
2. UK COMINT PEACETIME COLLABORATION WITH FOREIGN GOVERNMENT, EXCEPT UK, CAN OR AUS CLASSIFIED SECRET.
3. INTELLIGENCE FROM CRYPTO SYSTEMS, 1 SEPTEMBER 1931 - 2 SEPTEMBER 1945 NOT REVEALING SPECIFIC SYSTEMS INVOLVED, EXCEPT[1].
4. CATEGORY III CODEWORDS (CURRENT AND OBSOLETE)

SECRET

1. INTERCEPT ASSIGNMENTS, EXCEPT[1]
2. INTERCEPT D/F PLANS, EFFECTIVENESS AND ORGANIZATION
3. DETAILS OF TRAFFIC ANALYSIS OF ENEMY COMMUNICATIONS DURING WORLD WAR II.
4. DETAILS OF CRYPTANALYSIS OF LOW GRADE ENEMY MILITARY CRYPTOSYSTEMS DURING WORLD WAR II
5. COMINT COLLABORATION BETWEEN US, UK, CAN, AND AUS.
6. CATEGORY II CODEWORDS (CURRENT AND OBSOLETE).

1. FOR EXCEPTIONS, SEE CITED PARAGRAPHS ON PAGE INDICATED.

Inclosure to Appendix to
NSA Regulation No. 121-7
dated 8 April 1955

~~HANDLE VIA COMINT CHANNELS ONLY~~