

~~CONFIDENTIAL~~

NSA CIRCULAR
NUMBER 41-3

NATIONAL SECURITY AGENCY
Washington 25, D. C., 9 August 1954

EFFECTIVE UNTIL RESCINDED OR SUPERSEDED

NSA STANDARDS FOR COMINT TRAINING
IN THE MILITARY DEPARTMENTS

	<u>SECTION</u>
SUPERSESSON	I
PURPOSE	II
GENERAL	III
SCOPE AND FORMAT OF STANDARDS	IV
IMPLEMENTATION	V
COMPOSITION OF PROGRAMS OF INSTRUCTION	VI
LIAISON	VII

SECTION I - SUPERSESSON

This Circular supersedes NSA Circular Number 41-3, dated 9 March 1954.

SECTION II - PURPOSE

The purpose of this Circular is to describe the scope and format of National Security Agency Training Standards and to prescribe the procedures for the implementation of NSA Training Standards in the Military Departments.

SECTION III - GENERAL

1. NSA Training Standards will outline and prescribe the minimum scope of COMINT training courses conducted by the Military Departments.

a. The term "COMINT training" as used herein is understood to embrace all training in the fields of cryptanalysis, traffic analysis, regular or specialized intercept techniques, and in ancillary communication intelligence fields including language.

2. NSA Training Standards will be issued for all formal training and apprentice training in COMINT conducted by the Military Departments.

a. The term "formal training" as used herein is understood to mean training in which most of the instruction is conducted in a classroom.

~~CONFIDENTIAL~~

NSA CIRCULAR NO. 41-3

9 August 1954

b. The term "apprentice training" as used herein is understood to mean training which is normally performed under the direction of the Service commander concerned in the station to which the trainee is assigned, which has as its essential purpose the familiarization of the trainee with his job, and which has a definite plan, schedule, and duration.

SECTION IV - SCOPE AND FORMAT OF STANDARDS

1. NSA Training Standards will be written in terms of minimum requirements. Where these requirements are stated in number of hours to be devoted to a major phase of study, this number of hours represents the amount considered by the concensus of persons fully experienced in the particular problem as the minimum time likely to be needed by the average student to acquire the desired proficiency. These phase lengths, therefore, are for guidance. However, any significant reduction in the number of hours to be devoted to any phase by any individual Service must be requested of the Director, NSA, and must be accompanied by a detailed justification.

2. NSA Training Standards will normally consist of most of the following items:

- a. Effective date of the Standard.
- b. Course title or subject.
- c. Pertinent Service job codes or occupational specialties.
- d. Objective.
- e. Prerequisites.
- f. Subject matter or phases to be covered.
- g. Methods of instruction.
- h. Suggested minimum length.
- i. Objective standard (if possible to prescribe).
- j. Means of verifying achievement.
- k. References.
- l. Classification of course content and materials.
- m. Special instructions (if any).

~~CONFIDENTIAL~~

NSA CIRCULAR NO. 41-3

9 August 1954

SECTION V - IMPLEMENTATION

1. NSA Training Standards will be issued in provisional form for each course of training. Provisional Standards submitted to the Service Cryptologic Agencies may be accompanied by a memorandum discussing the factors which were considered in their preparation.
2. Within 45 days after the issuance of each Provisional Standard, Service Cryptologic Agencies affected will send to the Director:
 - a. Comments and recommendations for revision, if any.
 - b. An estimate of when the requirements of the Standard can be met. Major obstacles to implementation will be reported to the Director, who will provide assistance as appropriate.
3. The NSA Training Standard will then be promulgated in final form, and the Service Cryptologic Agencies concerned will, upon receipt of an NSA Training Standard, submit as soon as practicable to the Director a course outline based on the Standard. Programs of Instruction, prepared in the form outlined in the following section, will be submitted subsequently as promptly as possible.
4. All reports submitted in compliance with this Circular should cite RCS NSA 301.

SECTION VI - COMPOSITION OF PROGRAMS OF INSTRUCTION

1. Programs of Instruction to be forwarded to the Director as required in Section V will include at least the following items, prepared along the general lines indicated:
 - a. Cover Sheet. The cover sheet will show the name of the course to which the Program applies and will, if possible, indicate the pertinent occupational specialty and Service job code. It will also show the date on which the program was approved by the appropriate Service authority.
 - b. Preface. The preface will contain a concise statement of the objective of the course, a list of the prerequisites to the course, and a statement of the length of the course expressed both in number of calendar weeks and in number of hours.
 - c. Summary. The summary will consist of a tabulation of the titles of each major unit of academic instruction in the course, each such unit being accompanied by a statement of the hours spent thereon.

~~CONFIDENTIAL~~

NSA CIRCULAR NO. 41-3

9 August 1954

d. Detailed Breakdown. Each major unit will be further subdivided into the specific subjects of which it is composed. To make this portion of the Program of Instruction as useful and informative as possible, an attempt should be made to subdivide each unit of instruction into the smallest subunits which are still meaningful. With but few exceptions, no unit comprising more than 40 hours should be left undivided in this portion of the Program. For each specific subject the following data, constituting a subject schedule, will be presented in tabular form:

- (1) Subject of each lesson.
- (2) Time allotted and type of instruction. The following symbols will be used: L for lecture, C for conference, D for demonstration, TF for training film, PE for all types of practical exercises, and E for all types of examinations.
- (3) A concise but informative statement of the scope of instruction and the nature of any demonstration, practical exercise, or examination prescribed.
- (4) References. A list of the texts and training aids actually provided as student study references; and a list of the specific practical exercises and examinations provided for use by students.

2. Because the detailed breakdown of the units is the most useful portion of the Program of Instruction, an example of such a breakdown is attached as Appendix.

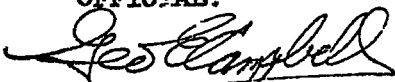
SECTION VII - LIAISON

Representatives of the Director will make frequent visits to the Service Cryptologic Agencies concerned with COMINT training to observe the functioning of training programs and to offer assistance in setting up training or in resolving problems pertaining to COMINT training.

BY COMMAND OF LIEUTENANT GENERAL CANINE:

L. H. FROST
Rear Admiral, U. S. Navy
Chief of Staff

OFFICIAL:



GEO. E. CAMPBELL
Colonel, AGC
Adjutant General

Incl:
Appendix

DISTRIBUTION V plus - 4 -
TNG (10)

~~CONFIDENTIAL~~

APPENDIX

Example of a detailed breakdown of a unit of instruction, as outlined in paragraph 1d, Section VI:

UNIT NO. 1

MONOALPHABETIC SUBSTITUTION SYSTEMS

(200 hours)

Subject	Hours and type	Scope of instruction	References
Fundamental Principles	16 L, D, PE	Basic cryptologic terminology and procedures; the monographic phi test.	Chapters I through IV, NSA text "Military Cryptanalytics, Part I". Lesson 1, NSA Problem Book, same title.
Unilateral Substitution	20 L, D, PE	Cryptography and cryptanalysis of unilateral substitution with standard and mixed cipher alphabets; the probable word method; completion of the plain component sequence.	Chapters V and VI, NSA text "Military Cryptanalytics, Part I". Lesson 2, NSA Problem Book, same title.
Simple Multilateral Substitution	24 L, D, PE	Cryptography and cryptanalysis of multilateral substitution with single-equivalent cipher alphabets; elementary cipher teleprinter.	Chapter VII, NSA text "Military Cryptanalytics, Part I". Lesson 3, NSA Problem Book, same title.
Variant Substitution	28 L, D, PE	Cryptography and cryptanalysis of multilateral substitution with variants; use of isologs.	Chapter VIII, NSA text "Military Cryptanalytics, Part I". Lesson 4, NSA Problem Book, same title.
Polygraphic Substitution	16 L, D, PE	Cryptography and cryptanalysis of representative polygraphic systems; 4-square, 2-square, and Playfair cipher systems; the digraphic phi test.	Chapter IX, NSA text "Military Cryptanalytics, Part I". Problem 1 from each of Lessons 5, 6, and 7, NSA Problem Book, same title.
Monome-dinome Substitution	24 L, D, PE	Cryptography and cryptanalysis of monome-dinome substitution; use of isologs.	Chapter X, NSA text "Military Cryptanalytics, Part I". Problems 1 through 5, Lesson 8, NSA Problem Book, same title.
Syllabary Squares & Code Charts	40 L, D, PE	Cryptography and cryptanalysis of syllabary squares and code charts; coordinate recovery; square recovery; use of bulk messages.	Par. 80, NSA text "Military Cryptanalytics, Part I". Lesson 9, NSA Problem Book, same title.
Foreign Language Ciphers	32 L, PE	Solution of a few monoalphabetic substitution ciphers in which the underlying plain texts are in a foreign language; introduction to foreign language cryptolinguistics.	NSA text "Military Cryptanalytics, Part I". Course BETA, Section 86-30, "Cryptanalyst's Manual".

Appendix to NSA Circular
41-3, 9 August 1954