

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
 HEADQUARTERS ARMY SECURITY AGENCY
 WASHINGTON 25, D. C.

CSGAS-70
 SUBCOMMITTEE REPORT NO. 22

14 February 1949

MEMORANDUM FOR THE ARMY SECURITY AGENCY TECHNICAL COMMITTEE

Subject: Initiation of D/A Project No. 29-66-030, NC-4 Mark II and
 Alphabetic Substitution Device

1. REFERENCES:

a. IRS from Chief, Machine Branch to Chief, Research and Development
 Division, dated 6 January 1949, Subject: NC-4 Mark II.

b. IRS from Chief, Machine Branch to Chief, Research and Development
 Division, dated 17 January 1949, Subject: Military Characteristics of the NC-4
 Mark II and Alphabetical Substitution Device.

2. DISCUSSION:

a. Agencies Concerned:

- (1) Cognizant Agency: Navy
- (2) Directing Agency: Navy
- (3) Requesting Agency: Army Security Agency and Navy
- (4) Participating Agency: Army Security Agency
- (5) Coordinating Agency: Navy
- (6) Other Probable Interested Agencies: USAF

b. Purpose:

The purpose of Project No. 29-66-030 is to develop an improved
 basic machine and an auxiliary device for performing numeric and alphabetic
 substitutions and other operations in cryptology. This equipment will be
 operated by CSGAS-92.

c. Description:

The NC-4 Mark II will be analogous to the commercial IBM reproducer
 except that there will be an additional set of 80 brushes in each feed and a
 coordinating feature which will control feeding depending upon the reading in
 the two feeds. In addition it will be designed to permit attachment of various
 special devices such as the alphabetic substitution device for controlling
 its operations. The alphabetic substitution device will permit the encipher-
 ment or decipherment of 1 to 5 element units at the rate of 100 units per
 minute. The substitution device will have a 32 x 32 matrix which will be
 completely flexible to accommodate any set of 32 32-element sequences.

Declassified and approved for release
 by NSA on 08-07-2013 pursuant to E.O.
 13526

CONFIDENTIAL

d. Related Material:

The NC-4 Mark I Machines now in use by CSGAS-92 were built for the Navy during the War and are badly in need of replacement. Their design does not permit many essential functions which will be incorporated in the NC-4 Mark II.

e. Development History and Status:

A project has been set up by the Bureau of Ships for design and construction of the NC-4 Mark II and for certain auxiliary equipment as indicated in the specifications attached as an Exhibit. Design work has been completed by the International Business Machines Corporation and construction is underway.

f. Proposed Development:

This project will be conducted under contract negotiated by the Navy, to which the Army Security Agency will transfer funds.

- (1) Phases of the project include development and engineering and service tests.
- (2) Four service test models of the NC-4 Mark II will be required and one service test model of the alphabetic substitution device will be required. The service tests will be made by CSGAS-92 and Navy.
- (3) Priority 1C is recommended, within the terms of Par 3a(2)(c) of War Department Circular 71, 18 March 1947, because of the intended operational use.
- (4) The estimated cost of this project to the Army Security Agency is \$74,800.
- (5) Development will be completed in approximately 18 months.

g. Security Classification:

- (1) The equipment while under development will be classified **CONFIDENTIAL**.
- (2) This equipment will be considered in the "limited" category.
- (3) Cryptographic clearance will not be required for personnel concerned in the development.

3. RECOMMENDATIONS:

The Subcommittee recommends that Project 29-66-030, NC-4 Mark II and Alphabetic Substitution Device, be established, classified as Development Type, Service Test Type, and assigned a priority of 1C.

4. EXHIBITS:

A. Proposed Military Characteristics.

5. COORDINATION:

Coordination was accomplished with the following agencies:

Navy

USCRAD



LEO ROSEN
Chairman, Cryptologic
Subcommittee, ASATC

1 Incl.
Exhibit "A"

EXHIBIT "A"

Proposed Military Characteristics for NC-4
Mark II and Alphabetic Substitution Device

I. General Information

A. Objective

1. The object of this development is to produce (a) a basic machine similar in nature to the present NC-4 (a type of presensing punch) but having increased capacity of control and computation, more flexibility and improved accuracy and (b) an alphabetic substitution device associated with the basic machine.

2. Equipment of the type described herein is required to expedite decipherment and to permit substitution operations of various types. In addition, other cryptologic functions, e.g., those involved in transposition solution and decoding, can be performed.

B. Functional Characteristics

1. The NC-4 Mark II shall have as its general functions:

- a. Transcription of information from one file of punched cards to another.
- b. Comparison of data between two files of cards in such fashion as to control both the feeding and punching of cards.
- c. Sensing of information for further analysis and punching the result of that analysis into the same card from which the source data was read.
- d. Control by basic machine of various auxiliary devices.

2. The alphabetic substitution device should be attachable to the basic machine and shall permit simultaneous decipherment or encipherment of 1 to 5 positions through a pluggable matrix having a capacity of 32 32-element alphabets.

C. Tentative Technical Considerations

1. The basic machine shall have a form analogous to the present IBM type 519 reproducer with the following principal differences:

- a. Three reading stations in the reproduce feed.
- b. Two reading stations in the punch feed, one preceding and one following the punch station.

- c. Coordinating feature which would permit a control of feeding in both feeds from reading of the cards. In addition, the coordinating feature shall permit control of punching and other functions of the machine.
- d. Provision for attachment and control of auxiliary devices.

2. The alphabetic substitution device shall have the following characteristics:

- a. A pluggable matrix permitting the plugging of 32 32-element alphabets.
- b. A choice of any 32 out of the 38 standard IBM codings for result punching.
- c. A choice of any 32 out of the 38 standard IBM codings to control the coordinates of the matrix.
- d. Ability to bypass the matrix whenever a special character representing a garble occurs in either or both key and cipher (or plain).
- e. Automatic checking features to insure accuracy of results.
- f. Capacity to operate from 1 to 5 positions for each card at the rate of 100 cards a minute.

D. This equipment shall be used at fixed stations.

E. The equipment shall be installed in fixed IBM installations of the Army Security Agency and other cryptologic agencies.

F. The weight of the equipment shall not exceed 125 lbs per square foot of bearing area. The maximum dimensions shall not exceed height 6 ft., width 4 ft., length 5 ft.

G. The desirable life expectancy of the equipment with reasonable maintenance shall be 5 years under either peace or war conditions.

II. Performance Requirements

A. Equipment shall conform to the same standards required for commercially produced IBM machines.

III. Operations and Maintenance Consideration

A. Equipment shall be capable of continuous operation for 20 hours a day.

B. The basic machine and auxiliary device shall require no more than one operator and shall be maintained and serviced by the same personnel who maintain and service other IBM equipment.

C. Provision for Field Maintenance.

1. Requirements for field maintenance shall be similar to those for other IBM equipment.

IV. Physical Characteristics.

A. Equipment design shall take into consideration simplicity of maintenance, maximum possible use of standard parts and other similar considerations normally involved in the design of IBM equipment.

B. The equipment shall operate from 110 volts 60 cycle single phase power supply.

C. This equipment shall be designed for use in Phase IV of air operations.

D. The construction in so far as ruggedness, temperature limits, etc. shall permit shipment to and installation at any fixed IBM installation of the Army Security Agency.