VF 408-13

ENCLOSURE B

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

Form to be used for the presentation of a cryptographic system, plan or device, to the Chief Signal Officer for an examination to determine its military value.

---

1. All cryptographic systems, plans, or devices received by, or officially referred to, the Chief Signal Officer will be given full and complete consideration.

2. All descriptions and data submitted will be considered confidential, but it must be understood that the submission of a cryptographic system, plan, or device or of any data applicable thereto does not obligate this office in any way, save to safeguard the secrecy of the disclosure.

3. It is to be understood that the submission of descriptions and data, and the perusal thereof by the War Department, will not, of itself, obligate the Government to enter into any financial arrangements with the applicant. No advance of funds can be made for the preparation of drawings, descriptions, or models, nor for the personal and traveling expenses of the applicant. Even though a device may initially appear to be practicable for military use, it may in certain instances be necessary to build one or more experimental models in order to determine definitely and finally whether or not the device is of such a nature as to justify its adoption as standard equipment. Such use will be considered as experimental only, and neither as constituting infringing use of a patented device, nor as such a use as to raise an implied contract in the case of a device patented or unpatented.

4. A statement of the claims alone made for a project is insufficient. It is essential that a complete plan and description be supplied of the manner in which it is proposed to accomplish these claims in actual practice. The submission of merely a single sample or even a few samples of cryptograms produced by the cryptographic system, plan, or device does not in any way permit a complete determination to be made of the military value of the system, plan, or device.

Note: This office desires to indicate that it fully appreciates the situation confronting the proponent of a cryptographic system when he is asked to submit a detailed explanation of his system. His hesitancy in disclosing what he deems to be the most important phase of his cryptographic system, without some safeguard satisfactory to him, is quite understandable.

Unfortunately, no safeguard can be given him. His position in the matter is identical with that of a chemist who wishes to dispose of a secret process or formula but who, when he is asked to disclose the details of his process or formula, must rely upon the integrity of those with whom he proposes to deal. For example, there are scores

of methods of producing a certain simple chemical; some of these methods are practical, but many of them are wholly impractical for large scale production. If an inexperienced chemist should offer what he believes to be a new method for producing this chemical, and would merely offer a small sample of his product, this would tell little or nothing about the value of his process from the point of view of practical, large scale production. His method may be new to him but it is much more probable that what he regards as a novel method has been known to chemical technicians as a laboratory curiosity for a long time, and has been discarded as wholly unsuitable for practical employment. But there is no way of finding this out until either a very painstaking, expensive, large scale production test under practical conditions is made side by side with the older, well-known methods, or the chemist is willing to disclose the details of his secret process.

To continue the analogy, the inventor of a cryptographic system, plan, or device may be of the opinion that he has devised a new, practical, secure method. He may offer only a small sample, or even several samples of his product. There are on the market and in practical use several other methods, all for the same purpose, all having undergone more or less successfully the test of practical usage. It is obviously impossible to make a test of the inventor's system alongside systems now in use, for the reason that not only would he have to prepare as many as 1000 or 2000 messages under conditions set forth by this office, in order to duplicate as nearly as possible the actual conditions under which cryptographic communication is conducted between large offices in the rear, or hundreds of small headquarters in the combat zone, but also this office has neither the personnel nor the time to devote to such a study as would be essential in the case of each of the many systems presented for consideration. The only other alternative open either to the inventor or to this office, if the former wishes an examination of his system for possible use in the military service, is for him to disclose the details of the system. Moreover, such a disclosure is essential in order that the system, plan or device meet the requirement set forth in Paragraph 7 of the accompanying Enclosure A.

5. Should a cryptographic system, plan, or device prove meritorious, the entire matter will be referred to the proper branch of the War Department for negotiations as to compensation.

6. A complete examination of a cryptographic system, plan, or device may involve a delay of one week or several months. Their submission in person is therefore not recommended on account of the added cost to the applicant for traveling and living expenses. The Chief Signal Officer cannot send officers or employees to examine any plans or models at the home of the applicant before the proposal has been submitted in writing and an examination has been made to determine its possible military value.

7. The Chief Signal Officer considers the project with a view to its value for military purposes only and does not attempt to pass upon its value for naval, diplomatic, or commercial use.

8. In submitting your cryptographic system, plan, or device for examination, please complete carefully the following questionnaire:

Date_____

(1) Your name:_____

(2) Your address:_____

(3) State briefly the particular point of novelty or superiority in your project, which is not found in other cryptographic systems, plans, or devices of today. (The degree of secrecy claimed as a result of the use of your project is not desired here.)

_____

_____

_____

(4) Is your project

(a) A system or plan requiring no apparatus?

(b) A device?

(5) Is your project

(a) In use?

(b) Worked out in detail on paper?

(c) An idea requiring development?

(6) In order to permit of a satisfactory examination, your system, plan, or device should be submitted as follows:

(Note: As these papers will become a part of the permanent files of this office and cannot be returned, copies only of all drawings and description should be supplied.)

(a) If it is patented, enclose a copy of the patent. If not enclosed, give the serial number of the patent.

(b) If patent application is pending, send a copy of the specification and prints of drawings.

(c) If not the subject of a patent or patent application, enclose a full, complete, and clear description and explanation, together with such sketches or drawings as may be necessary to enable a person not familiar with your ideas

to understand them. Sign and date all descriptions, explanations, and sketches.

(d) The description and explanation referred to above should consist of:

(aa) A detailed, complete statement of the basic cryptographic method.

(bb) At least one example of a plain-text message of a minimum of 50 words in good English; all the keys employed in the encipherment of this message; and the final cryptogram. A step-by-step, detailed description of how the plain-text message is converted into the cipher message must be included.

(cc) A minimum of three cryptograms, each being the enciphered version of the same plain-text message of at least 750 letters, in good English, the specific keys being different in each case. Neither the plain-text version of the cryptograms nor the keys pertaining thereto should be included.

(dd) A minimum of 20 cryptograms, each being the encipherment of a different plain-text message of at least 100 letters, in good English, the specific key being exactly the same for these 20 messages. Neither the plain-text versions of these cryptograms nor the keys pertaining thereto should be included.

(Note: Before submitting your messages, it is requested that a careful check be made of them in order to ensure that no errors in enciphering are present.

Additional messages as may be warranted by the special circumstances applicable to each case under investigation may be called for later by the Chief Signal Officer, if found necessary for an exhaustive study of your system, plan, or device.)

9. All correspondence in connection with this subject should be addressed to the Chief Signal Officer, War Department, Washington, D. C.

June 19, 1940