~~TOP SECRET~~

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

CSGAS-14

22 September 1949

MEMORANDUM FOR: GENERAL CLARKE

SUBJECT: Background of Policy in Regard to Making SIGABA Available to the British

1. a. To begin with, it is important to note that when the ECM-SIGABA was conceived, the basic premise or requirement which the U. S. experts had to meet was this: a cryptographic machine for military use must be designed so that its capture or compromise will not jeopardize the security of future communications enciphered by that machine. The reason for this requirement is not only that research, development and testing of crypto-equipment is expensive and time-consuming, but also that during a war there is no time to repeat the research, development, testing, installing, and training of personnel each time a machine is lost, captured, or compromised. This requirement is certainly a logical one and the ECM-SIGABA fully met it when it was designed; it still meets the requirement despite the astonishing developments in the past 10 years in cryptanalytic machinery and techniques. All the top-level cryptologic technicians in both the Army and the Navy are absolutely sure that, in the present state of cryptanalytic technology, even if an enemy government with a good cryptanalytic organization had an ECM-SIGABA, the reading of communications properly enciphered by that machine is impossible without possession of the key which gives the exact "setting" of the crypto-elements for the day. In the minds of those technicians there never was and there still is no danger to U. S. communication security if the machine is lost or compromised and hence there can be no loss in security of U. S. communications if the ECM-SIGABA were disclosed and released to the British.

b. The problem as to whether the SIGABA should be disclosed and made available to the British is one which has confronted and been discussed by U. S. authorities ever since the equipment was introduced into service late in 1941. Although there was a high level decision to collaborate on cryptanalytic work, collaboration on cryptographic work was much restricted. (See Incl. 1.)

c. From the early days of our active participation in World War II, Combined communications between U. S. Navy and British Navy over the North Atlantic convoy routes were very much hampered by the slowness and unreliability of the cryptosystem provided by the British.

~~TOP SECRET~~

This consisted of a figure-code (British Naval Cypher No. 3) enciphered by additives. It was the only cryptosystem then available for Combined use. U. S. Navy technicians had some doubts as to the security of the system but these were minimized by the British. It was early in 1943 that the U. S. Navy obtained proof that high convoy losses were attributable to German solution of the British system and German reading of convoy traffic.

d. In the early part of 1942 Colonel John H. Tiltman, officer in charge of the Services Division of the British cryptologic organization (GC & CS), came to Washington to discuss U.S.-British collaboration, including cryptographic systems for Combined U. S. Army-British Army (and RAF) communications. Authority was granted to discuss with him the possibility of using the strip cipher device and Converter M-209 (Incl. 2). But the British did not think either of these suitable for the purpose. Though they had their TYPEX machine, they did not have enough of them for their own use, let alone enough to hand over to the U. S. for Combined communications. Besides, the U.S. experts did not think too highly of the TYPEX in comparison with the ECM-SIGABA and, furthermore, to adopt the TYPEX for COMBINED communications would mean that each U. S. headquarters would have to carry two large machines. The British knew we had a machine and were in heavy production. They therefore wanted the ECM-SIGABA and brought heavy pressure to bear upon U. S. high level authorities to disclose it in the hope of getting it released to them to replace the TYPEX and make it unnecessary for them to carry two machines. Apparently the effort to gain at least a look at the machine was successful because on 25 April 1942 verbal authority was granted to both Army and Navy representatives to show Col. Tiltman the machine. (See handwritten note at bottom of page 2 of Incl. 2.) A joint demonstration of the ECM-SIGABA was made in the Navy Department and the basic cryptographic principles were explained to Col. Tiltman. In return Col. Tiltman demonstrated the TYPEX machine to the Army representative, who had never seen it.

e. British pressure to get the ECM-SIGABA released continued. It is my distinct recollection that the resistance was much stronger in the Army than in the Navy at that time. This recollection is supported by a memorandum dated 9 July 1942 (Incl. 3) in which the President asked General Marshall to look into the matter of a more intimate exchange of information between the cipher experts of the U. S. Army and the British Army, implying that such an exchange was in effect between those experts of the U. S. Navy and the British Navy. The memorandum was referred to General George V. Strong, A.C. of S., G-2, who neatly side-stepped the issue. He was able to do this because the President's memorandum was not very clear and did not specifically mention the question of releasing the SIGABA. I am sure that this was the point at issue but I have no documents to support this part of my recollection. General Strong simply noted that "intimate exchange of technical cryptanalytic information ... appears to be quite satisfactory to both sides" and that studies and conferences pertaining to an exchange of cryptographic information had been in progress for about three months and would soon be completed.

f. The studies and conferences referred to above were those dealing with the development of the CCM. This was a compromise solution to the problem of a Combined machine and was a project largely initiated and completed by the U. S. Navy. However, before embarking on this project, U. S. Navy experts tried to convince higher Navy authorities that it would be better to release the ECM to the British than to make a third machine or an adaptor for the ECM to enable intercommunication with the TYPEX. In an undated memorandum (April 1942?), the chief of the Navy cryptographic unit recommended the release, pointing out the advantages and disadvantages (Incl. 4). His recommendation was disregarded. In a memorandum dated 16 September 1942 (Incl. 5), the Chief of OP-20 (Navy cryptologic organization) pointed out quite clearly to the Director of Naval Communications that "If our plan of war is to keep England from falling and to prosecute the war with all our national resources to a successful conclusion, our present policy /of withholding the ECM/ is unsound and should be reversed without delay." However, his recommendation was also disregarded and work continued on the development of the CCM. One of the forms which the CCM took was the CSP 1700. This is a machine built upon the ECM chassis but with only five rotors. (It is similar to Army's SIGROD.) The British were provided with quite a number of CSP 1700 machines during the war. Whoever knows the cryptographic principles of the ECM-SIGABA and has a CSP 1700 can build an ECM easily enough.

2. The CCM proved to be fairly satisfactory as a solution to the problem of Combined communications but British pressure to get the ECM-SIGABA continued. In 1944 there was another drive on, because of some doubts as to the security of the CCM. But the U.S. attitude became even more firm and strenuous endeavors were made to prevent the British from seeing the machine. Joint regulations had been adopted (Incl. 6) and it was agreed that at no time would the SIGABA be put aboard a British vessel or in a British headquarters

except under custody of a U.S. Liaison team. These regulations were carefully observed but in at least one instance a failure occurred (Incl. 7), and there was good opportunity for the British to study the equipment in detail, for not only was the machine available but also complete instructions, etc. There may have been several other opportunities for learning details about the machine, but it is difficult to document them. A copy of a document (SIGKKK) giving complete details and drawings pertaining to the SIGABA was lost in Burma and never recovered. (See Incl. 7a.) This much we do know and can document: In the Combined conferences held in the spring of 1947 with a view to replacing or improving the CCM, the British frankly admitted that they not only understood the basic cryptographic principles of the ECM but also had incorporated them in a new machine for radioteletype communications. They explained their understanding of the cryptoprinciples and their explanation was correct.

3. a. Early in 1947 the British officially raised the question of a replacement for the CCM, stating that the present CCM was not secure enough for the Combined communications of another emergency. They sent Capt. Wilson to Washington to discuss the matter (Incl. 8). Prior to holding Combined conferences, there was a Joint meeting to arrive at a U. S. position in the matter.

b. The Joint meeting was held on 23 Jan 47 and it was decided that the first meeting with the British would be confined solely to a discussion of the CCM and that there would be no discussion whatsoever as to the possible use of the ECM (Incl. 9). On 28 January 47 the first Combined conference was held. It was at this meeting that Capt. Wilson disclosed that they knew the cryptographic principles underlying the ECM and would like to embody them in a new CCM but if the U. S. insisted on withholding the ECM they would like to present a wholly new idea. The British did not want to disclose their idea at that meeting, which then adjourned to allow U. S. representatives to confer among themselves and perhaps to get some indication from higher authority as to whether a policy decision would be made regarding the long-term retention or scrapping of the ECM principles (Incl. 10). In the subsequent Joint discussions the Army maintained the view that in view of all the presently-known facts it would be to the advantage of all concerned to let the British have the SIGABA. But despite all the arguments the Army representatives could present to the then Director of Naval Communications, he remained adamant against disclosure. It happened that during one of these Joint discussions in the Director's office in the Navy Department, Capt. Wilson was in the building and was asked if he would be willing to disclose the radically new British idea for a new cipher machine without any strings attached to his disclosure. He stated his willingness to do so (Incl. 11). It was thereupon agreed by the Army and Navy representatives in Joint session not to go to higher authority with the question of a possible change in policy but to see first what the British had to offer. On 21 February in a Combined meeting (Incl. 12) the British disclosed the principles of their proposed new cipher machine, which they called the RM 26. On 25 February at a Joint meeting the RM 26 was discussed and found to be wanting in practicability. On 28 February at a Combined meeting the U. S. position was stated in writing (Incl. 13) and it was made clear that the U. S. found it impossible to embark upon the development of a new CCM based upon the principles of the RM 26.

c. In view of the impossibility of getting the Navy to recede from its position on the matter of disclosing the ECM the Army had agreed to continue to withhold the ECM-SIGABA from the British and to collaborate with the Navy and the British in attempts to improve the present CCM. A Combined report of the discussions was drawn up and agreed upon at a Combined conference on 4 March 1947 (Incl. 14). One of the important points of the agreement was that Combined security regulations would be established. (This has been done.) An Army report of the Combined and Joint meetings was made to the Chief of Staff (Incl. 15) and likewise a Navy report was filed by Admiral Stone to the Chief of Naval Operations (Incl. 16).

d. Experimental work, conducted almost entirely by Navy, to improve the CCM was continued throughout 1947 and for a time Army was hopeful of good results because of Navy optimism concerning the outcome. There also were some Joint meetings and discussions during that year (Incl. 17). But progress was very slow and the British were getting impatient. Almost a year had gone by and still there was no improved CCM nor any signs that one was about ready to be submitted to them for study. On 16 February 1948 there was another Joint meeting (Incl. 18) to discuss a new British paper (Incl. 19) on the subject. It summarized and presented a rather dark but accurate picture of the situation as to the possibility of improving the CCM and concluded that "every effort should be made to reach agreement with U. S. authorities in the design and production of a brand new cipher machine for Combined purposes." There were Joint meetings and discussions throughout 1948 (Incl. 20) but little further progress was made. About the only outcome of Navy's experimental work was the production of a modified CCM which they called the BCM. The modification principally consisted in making two of the five rotors step backward; there was also a change in the order in which the rotors stepped. These brought some improvement in security but in Army's opinion the additional security was not too important. The Army representatives felt that it certainly would not satisfy the British, to whom the proposed modifications had not yet been communicated, and who were still waiting for an answer to the question raised early in 1947. Also, the idea of backward stepping of two rotors was a feature of the Navy's CSP 2900, a modification of the ECM-SIGABA and the Army pointed out that one of the Navy's own motives for producing the CSP 2900 was to have something that the British would not know about in connection with the ECM-SIGABA. Therefore, to disclose the BCM would militate against the idea that the CSP 2900 would be wholely unknown to the British.

e. In the meantime the British had been doing some work in the development of their RM 26 machine. But by the end of 1948 or early in 1949 it had become apparent to them that the U. S. experts had been correct in their contention that the RM 26 was impractical from an engineering point of view and further work on this machine was abandoned. Two full years had gone by and they had neither a new machine of their own nor an improved CCM for Combined communications.

f. Therefore, the British decided to reopen once more the question of releasing the ECM-SIGABA. In May 1949 they filed a paper (RDC 5/87) and in July they filed a modified paper (RDC 5/99) on the subject.

g. The British JCS paper was referred to the Joint Security and Cryptographic Panel of the Joint Communications and Electronics Committee for study and recommendation. The opinion and action of the Panel is summarized in Incl. 21. It is important to note that the Panel was unanimous in wishing to recommend acceptance of the 2d British proposal--release of the ECM.

4. To summarize my own opinion:

a. The Navy has consistently taken and has more or less stubbornly adhered to a position against disclosure, even when it became clear that the British knew the basic principles. The Navy felt and apparently still feels that there is security value in withholding the engineering know-how. But even that has become a weak argument since the British have had CSP 1700 machines. If the British wanted to "break faith" with U. S., they could build ECM's without our knowledge or permission. It is my assumption that they do not wish to do this on such a basis; also, it is possible that they do not wish to build the machines themselves--it is possible that they may want to buy them from Teletype Corporation in order to avoid a great and unnecessary research and development expense. That would be logical from the British viewpoint. Moreover, they know that even if they should secretly build ECM's for themselves, this would not solve the problem of Combined communications. Sooner or later they would be forced to tell the U. S. that they have their own ECM's--and the "cat would be out of the bag." It seems to me that they have looked ahead and have seen what embarrassment there would be in such a course and have wisely decided to try once more to get the ECM without subterfuge and to legitimatize their possession of knowledge of its principles so that they can make use of that knowledge legitimately.

b. The Army had originally and up to the early part of 1947 shared the Navy viewpoint. But after the Combined conferences in the spring of 1947, the Army changed its view and was willing to release the SIGABA to the British. It only concurred with the Navy in the hope that Navy contentions that the CCM could be satisfactorily improved would be sustained. Since those contentions have not been sustained, the only logical course is to accept the 2d British proposal, viz., <u>officially</u> to release to them the cryptographic principles of the ECM-SIGABA and let them have full details of its construction. They will then be in a position to use this knowledge legitimately and without embarrassment, and steps can then be taken very speedily to arrange for Combined communications in a way that will be mutually satisfactory.

William F. Friedman
WILLIAM F. FRIEDMAN
Special Assistant

21 Incls