

~~SECRET~~

SPSIS-3

27 September 1943

MEMORANDUM For: Colonel Corderman

SUBJECT : Recommendations for Legion of Merit and
Medal for Merit Awards

1. After much thought and careful study of the memoranda sent me by Branch Chiefs on the subject, the achievements deemed by me to be sufficiently noteworthy to warrant making recommendations for award are set forth in the following paragraphs.

2. A Branch Achievements.—Major Sheetz has drawn up a rather detailed memo outlining what his branch has accomplished. I am, however, not sufficiently acquainted with his activities to pass any judgement and will therefore leave his memo for your consideration.

3. B Branch Achievements.—a. Lieut. Colonel Cook has drawn up a brief memo indicating certain noteworthy achievements and the names of those to whom most credit is due. However, since he has been chief of that branch for such a short time, Colonel Cook indicated to me that he knows too little about the various past achievements to be certain that he has treated them adequately, and that I was to feel free to make any changes or additions I deemed desirable. This I have done, in connection with his memo and I therefore submit the following items for your consideration.

b.(1) I regard the Japanese "Purple" machine and the underlying system to have been by far the most difficult cryptanalytic problem successfully handled and solved by any signal intelligence organization in the world and, so far as AH is concerned, this has been and still is the most important source of strategically valuable, long-term intelligence. The accomplishment was by no means the work of one or two people

Daily

Declassified and approved for release by NSA on 11-05-2014 pursuant to E.O. 13526

~~SECRET~~

~~SECRET~~

but the result of the cooperative labors of a competent team working under my direction for a period of over 18 months. (A paper entitled "Preliminary Historical Report on the Solution of the 'B' Machine" is on file and available for your perusal.) My principal assistants were Mr. (now Major) Frank B. Rowlett, Mr. Robert E. Ferner, Mrs. Genevieve Grotjan Feinstein, Mr. Albert W. Small, and Mr. Samuel S. Snyder. To Miss Mary Louise Prather credit should be given for the careful keeping of the records and the index of all messages and it was as a result of her painstaking attention to detail that a paraphrased message was found which formed a very important link in the solution.

(2) An immediate result of the solution was the possibility of constructing a machine to duplicate what the Japanese machine was doing. This was accomplished without the benefit of any information whatsoever in the way of captured or pilfered drawings, blueprints, etc., but solely from an understanding of the cryptographic principles underlying the system, so that a machine could be constructed. For the construction of the first and later models the major share of credit is due Mr. (now Major) Leo Rosen and Mr. (now Major) Frank B. Rowlett.

(3) The Purple System has undergone some changes since its inception. For keeping abreast of those changes and following them cryptanalytically step by step, so that we have never been without the ability to read Purple messages for more than a very few days at any time, the major share of credit belongs to Miss Mary Jo Dunning, and to Mrs. Feinstein, as well as to Major Rowlett, and Messrs. Ferner and Small. Since December 1941 the major responsibility for the continuity of cryptanalytic operations in connection with the Purple system has been very ably discharged by Captain E. Dale Marston.

c. I regard the solution of the Japanese Military Attache System of 1941-43 as being next in importance to the Purple, from the point of view of the amount and value of the intelligence it has yielded and the difficulties involved in the solution. For this achievement the largest share of credit is due Colonel J. H. Tiltman of GC & CS, who made the initial break into the system, and for this, as well as for his other achievements it is recommended that his name be forwarded as deserving of the Legion of Merit award. So far as AH personnel are concerned, the major share of credit for the JMA solution belongs to Mr. Samuel S. Snyder and Mr. Frank Lewis. Others

~~SECRET~~

who materially assisted in the solution are Mrs. J. R. Thompson, Mr. (now 2d Lieut.) Karl Elmquist, and Messrs. Edward Christopher and C. Ronald Cassity.

d. The next most valuable source of intelligence was the Japanese transposed code system known as "J-18" and "J-19". Its solution represented a high cryptanalytic achievement, for initially the system appeared to be impregnable. For the development of the techniques and procedures in solution and for the mechanization of those techniques and procedures major credit belongs to Major Rowlett and Messrs. Ferner and Small. For continuity in cryptanalytic operations, credit belongs to the group under the direction of Colonel J. A. Verkuyl, including Mr. Eugene Waltz, Mr. William O. Bryan, Mr. Joseph S. Petersen, Jr., Mr. (now Sgt.) George Hurley, Miss Isabel M. Murdock, and Miss Elizabeth Stevens.

e.(1) The next most noteworthy cryptanalytic achievement of B Branch, in my opinion, is the solution of the German diplomatic system known as the "Keyword" or "Floradora" system. For sheer perseverance and bulldog determination, clever analysis, ability to detect and to employ minute clues leading to the ultimate breakdown of the system, after GC & CS had given up the problem as hopeless, and for organizing the procedures so that the very large amount of work involved could be expeditiously handled, the major share of credit belongs to Lieut. Colonel Solomon Kullback. His principal assistants whose contributions deserve mention are: Mrs. Delia Sinkov, Mr. Frank W. Lewis, Major Leonard Bickwit, Captain Roy D. Johnson, 1st Lieut. Leonard Seidenglanz, and Master Sergeant William Lutwiniak.

(2) For organizing the vast amount of IBM work involved and for devising new procedures for facilitating the operations in connection with the German Keyword System, Captain Stephen Dunwell deserves particular mention.

f. The very recent cryptanalytic successes in Japanese Army systems will undoubtedly prove to be of the utmost importance within a short time. For these successes the major share of credit belongs to Lieut. Colonel Solomon Kullback, Mr. Frank W. Lewis, T/4 Carl D. Mead, Mrs. Delia Sinkov, and Mr. Albert W. Small, who was in charge of direction of the problem up to 15 March 1943. Also, the cooperation and contributions of Lieut. Colonel Abraham Sinkov and Major H. L. Clark of the Central Bureau in this field have been important in the success achieved.

~~SECRET~~

g. Noteworthy also are the following achievements:

(1) Cryptanalysis of the Hagelin Cryptograph as used by the Finnish and Swedish Diplomatic Services. For this excellent cryptanalytic accomplishment the following persons deserve mention: Mr. Robert O. Ferner, Captain John N. Seaman, Technical Sergeant George H. Vergine, Dr. Martin Joos, 1st Lieut. William P. Bundy, 1st Lieut. Walter J. Fried, and 1st Lieut. Arnold I. Dumey.

(2) Solution of meteorological messages for North African Invasion Forces, for which the major portion of credit goes to Captain Edmund Wrigley.

(3) For organizing the IBM section the major portion of credit belongs to Major Perry Molstad; for devising new applications of those machines for cryptanalytic purposes, Captain James B. Greene and Captain Stephen Dunwell deserve special mention. For supervising the work in the IBM rooms and for loyalty to duty, industry, conscientiousness, and understanding of the problems of the employees supervised, much credit belongs to Master Sergeant John P. Hassett, Miss Delores Ekberg, and Messrs. Ulrich Kropfl and Charles Ehrmann.

h. None of the cryptanalytic achievements of B Branch in connection with Japanese diplomatic systems would have been useful had it not been for the excellence of the contribution made by the principal Japanese translators. In particular the work of Mr. John B. Hurt and the late Mr. Paul S. Cate deserve special mention in connection with the solution of the Purple system. Mr. Hurt has been since then ably assisted by Messrs. Gerhard, Nelson, Millard, Zaugg, Benson, Buchanan, and Faust, all of whom deserve mention.

4. C Branch Achievements.--a. Colonel Allsopp has drawn up a memo indicating certain noteworthy achievements and the names of those to whom most credit is due. However, since he has been chief of that branch for such a short time, Colonel Allsopp asked Lieut. Colonel Cook, former Chief of the branch, to assist him, and the memo submitted represents their joint work. But in view of the fact that there were, in my opinion, several deficiencies in the memo as submitted, I talked with both Colonel Allsopp and Lieut. Colonel Cook and pointed out items which I regarded as worthy of mention and which neither of them had full cognizance of. With their approval I have only used the list submitted by Colonel Allsopp as a general guide and submit the following items instead.

~~SECRET~~

~~SECRET~~

b. Cryptographic Developments.—Several of these are worthy of note:

(1) Converter M-134A.—This was the first automatic cryptograph developed by the Signal Corps and was the result of my invention (see U.S. Patent Application Serial No. 682,096, filed 25 July 1933, complete assignment to War Department by William F. Friedman). This machine was successfully employed for several years for highly secret and confidential communications between Washington, Panama, Hawaii, Philippines, and London (Military Attache's office). A number of these were also issued to the State Department for communications between the Department in Washington and our Embassy in London, and are still in heavy use between those two points. A number of them were also issued to the Office of Strategic Services and are now used for communications between OSS offices in Washington, London, Cairo, and Casablanca. Improvements recently made, by the addition of Keying Mechanism M-299, which replaces the key-tape transmitter by an automatic controlling device, places the machine on better footing cryptographically than any other machine now in existence, not even excluding Converter M-134C. However, because mechanically and electrically these machines are not too satisfactory they are being recalled from service, for special usage to be determined later.

(2) Converter M-134C.—Converter M-134A, which employed key tapes for controlling the displacements of the cipher rotors, was later superseded by Converter M-134C, in which the tape is eliminated and the displacements of the cipher rotors are erratically controlled by a sequence generated by a separate set of control rotors. The principle of using a rotor as a key generator was the invention of Mr. (now Major) Frank B. Rowlett. The reduction of this principle to practice and the design of the various elements entering into Converter M-134C was the joint work of Major Rowlett and myself (see U.S. Patent Application Serial No. 70,412, filed 23 March 1936, complete assignment to War Department by Frank B. Rowlett and William F. Friedman.) The importance and value of Converter M-134C in the conduct of the war hardly needs emphasis here. Since funds were available to the Navy soon after our invention, the first model of the machine itself was produced under a Navy contract in 1940, the two services collaborating in the final design, however, Converter M-134C now forms the backbone of all the secret and confidential communications of both services, including the Air Forces, the Coast Guard, and the Marine Corps.

~~SECRET~~

~~SECRET~~

(3) Converter M-228.—The necessity for providing automatic encipherment and decipherment for tele-type communications was recognized a number of years ago. The invention and design of Converter M-228 was the result of the joint work of Major Rowlett and myself (see U.S. Patent Application Serial No. 443,320, filed 16 May 1942, complete assignment to War Department by the inventors). These machines are highly useful for secret and confidential land-line tele-type communications; at present it is also used for confidential radio communications.

(4) "Zero Machine".—Early in 1942 a need developed for speedy intercommunication between X and Y (names furnished on request). A special project was set up and the first "auto-sigaba" produced by contract with the Western Union Cable Co. The design of the cryptographic apparatus was worked out by Major Rosen and myself. The system has worked and is working very satisfactorily, large volumes of traffic now being handled over this circuit.

(5) Converter M-325 and M-294.—These will be discussed under E Branch heading.

(6) Cipher Device M-138.—The cryptographic systems employing this device has served for a number of years as the principal means of secret and confidential intercommunication among the War Department and the many posts, camps, and stations within the U.S. It is still serving in this capacity and in addition it is the secondary or back-up system for use when the automatic cryptographic machines are out of commission. For developing the present form of the device and the system of employing variable strip alphabets in connection with it, major credit belongs to Mr. William F. Friedman, (see U.S. Patent Application Serial No. 300.212, filed 19 October 1943).

c. Cipher Machine Section.—The Cipher Machine Section organized and supervised schools for the training of maintenance men for all types of cipher machines. Graduates of these schools are at present maintaining U.S. Army cryptographic equipment in all theaters of operations. Improved maintenance methods have been developed. Certain production facilities were installed and put into efficient operation. The personnel who achieved the above were under the direction of Major Kenneth Kuhn.

~~SECRET~~

~~SECRET~~

d. Security Section.—The work done by this section in improving our own cryptographic techniques and finding sources of weakness has been of considerable importance. In particular, an extensive study was made of the converter M-209. Research was conducted on methods of solution of messages enciphered by this equipment. The techniques developed during this research were incorporated into the cryptographic system employing the converter thereby improving the security of the cryptographic system. The personnel who achieved the above were under the direction of PFC Paul R. Reimers.

e. Operations Section.—In the latter part of 1941 the undersigned began a study of all the cryptographic systems employed within the military establishment, with a view to their simplification and at the same time improving the overall security in cryptographic communication. This study resulted in the devising and development of the Cryptonet System, which more equably distributes the exceptionally heavy traffic load carried by individual War Department cryptographic systems. The Operations Section put the cryptonet system into effect without any disturbance in the continuity of cryptographic communication. A printing plant was put into operation. Cryptographic systems were produced and distributed throughout the world to a rapidly expanding list of holders. The personnel who accomplished these operations were under the direction of Captain Thomas R. Chittenden.

f. Procurement Section.—The procurement of all cryptographic equipment contracted for by the Signal Security Agency was supervised by the Procurement Section. Since all equipment was of special design it was necessary to supervise tooling as well as production. Due to shortages of critical materials the difficulties encountered were greatly increased. These obstacles were overcome and at the present time there are no back orders on hand for equipment and stock piles are being built up. The personnel who achieved the above were under the direction of Captain Russell H. Horton.

g. General.—For organizing C Branch, for successfully organizing the many activities therein conducted, and for his contribution toward establishing and maintaining cryptographic security in communication during several critical years, much credit belongs to Lieut. Colonel Earle F. Cook for his noteworthy achievement.

~~SECRET~~

~~SECRET~~

5. D Branch.—In a certain letter dated 3 January 1942, addressed to a cover name in Sweden and having as a return address a certain box office number in the Mexico City Post Office, there were found six microphotographs bearing information from the Japanese Naval Attache in Mexico and intended for the naval General Staff in Tokyo. They dealt with the reports of secret agents giving estimates of damage at Pearl Harbor and the Philippines. They also contained a forecast of the probable U.S. war plan in the Pacific for 1942. The discovery of these microphotographs and the revelation of their contents, was in my opinion, a noteworthy accomplishment. For this, and for the development of simplified and improved methods of microphotography, for use by our own agents, Lieut. Colonel A. J. McGrail is well deserving of mention for his noteworthy achievements.

6. E Branch.—a. Traffic Analysis.—Traffic Analysis was started as a new subject under the Signal Security Service in August of 1942. This operation in a new field has required the best in organization, attention to detail, foresight and imagination. It has had a pronounced effect on intercept coverage in supplying the necessary information for efficient assignment of tasks. It has also been of assistance to the cryptanalysts of B Branch and has supplied valuable order of battle data to the Assistant Chief of Staff, G-2. Captain Warren K. Hall has been associated with this work from its inception, and has been in direct charge during most of the time during which it has been conducted, much of the success enjoyed having been the result of his leadership and guidance. He is very ably assisted by Lt. Ralph J. McCartney, in charge of Japanese Army Traffic Analysis, and by M/Sgt. Stephen Wolf, who is the outstanding authority on Japanese Army Communications.

b. Communications.—The Signal Security Service communications have been rapidly expanded to meet the changing situation requiring speed as well as quantity of material handled. Only some eight months ago, the wire communications for intercept traffic were practically non-existent. At the present time there are six full time channels to our West Coast, radio communications for intercept traffic to Brisbane, Algiers, and Asmara, and arrangements for cable communication through BSC in New York to Ottawa and London. Over 6,000 messages a day are received by wire or radio means. An extensive communications net work exists for our own purposes. Most of this work has been accomplished by 1st Lieut. William F. Drees.

~~SECRET~~

~~SECRET~~

He has given these matters his personal attention and through his individual efforts he has made the communication system what it is in such a short time. In addition to this, Lieut. Drees is responsible for the organization and operation of a system for receiving and processing upwards of 10,000 messages per day. During the month of July 380,000 such messages were received by all means and processed.

c. Intercept personnel.—Shortly after the fall of Corregidor, two intercept operators, Lieut. Godfrey (then Sgt.) and Sgt. Shimmel were sent with a small quantity of equipment to Australia to test for a site to build another intercept station to replace the one lost in the Philippines. These two men never reached Australia. They were sent through Java and with the occupation by the Japanese went on to India with Major Martan. They established themselves in New Delhi, India and began intercept operations. These two men, acting on their own initiative, intercepted and shipped to the Signal Security Service a substantial quantity of Japanese Army material. They were also very helpful in submitting all data, notes on Japanese procedure and operating peculiarities which they were able to discover. As a result of their work, a twenty-man intercept station is being established at New Delhi. When the original mission of these men was changed by virtue of their going through Java into India instead of Australia, they could have given up the intercept project and returned to the United States, or attached themselves to some other signal unit for other work in India without warranting criticism. Their devotion to duty, courage and initiative led them to carry on despite difficulties and produce desirable and valuable results.

d. Other work.—(1) Although not a member of Signal Security Agency, Major Orla St. Clair, Officer in Charge, Signal Intelligence Service, Western Defense Command and Fourth Army, has performed outstanding work directly effecting the Signal Security Agency. He organized the traffic handling system for the three radio intelligence companies on the West Coast, and Two Rock Ranch, and assisted in arranging the performance of these radio intelligence companies along lines indicated by SSA. His tireless energy and personal attention to our needs has been of inestimable assistance. His spirit of cooperation was unusual.

(2) For reorganizing the intercept operations of SSA, for organizing the traffic analysis section from the

~~SECRET~~

~~SECRET~~

ground up, and for systematizing the very voluminous communications activities of the SSA, special credit belongs to Lieut. Colonel H. McD. Brown for a noteworthy achievement.

7. F Branch.—a. For the development, procurement, and installation, of the special rapid cryptanalytic equipment X-68003, and for training of a maintenance force for this equipment, the major share of credit belongs to Mr. S. B. Williams, of the Bell Telephone Laboratories and Major Leo Rosen.

b. Credit for the development of Converter M-294 and Converter M-325 belongs to the late Mr. A. H. Reiber and Mr. W. Zenner, of the Teletype Corporation of Chicago, Major Leo Rosen, and myself. The basic patent covering the cryptographic principles underlying Converter M-134C (Rowlett and Friedman) also cover Converter M-294. The basic principles covering the design and cryptographic principles underlying Converter M-325 were covered in a patent application of Mr. William F. Friedman (see Signal Corps Case SC-B-Sp-1, filed on 6 December 1941, with the R and D Branch, OCSigO.) *Schindler!*

8. HQ Branch.—Lieut. Colonel Slack has been consulted and he feels that this branch has made no achievements sufficiently noteworthy to warrant recommendations. However, it is thought that he is perhaps a bit too conservative. In my opinion, the work done in obtaining the necessary personnel for the large expansion which the SSA underwent from December 1941 to recent months, and in setting up the payroll and the complicated procedures in making deductions for retirement, victory tax, bond purchases, etc., is deserving of note. It is recommended that you consult with Colonel Slack on this matter and ascertain the names of those to whom credit is due.

9. Training Branch.—Major Edgerton has been consulted and he feels that this branch has made no achievements sufficiently noteworthy to warrant recommendations. It would, however, be false modesty if I failed to note the fact that the special texts in cryptography and cryptanalysis written by me during the past years were of immeasurable aid in the self-instruction of the large majority of the new workers, and that these texts have been in demand by other and allied services.

10. Personnel outside SSA.—a. The contribution of Colonel Tiltman has already been mentioned above. In addition,

~~SECRET~~

~~SECRET~~

in my opinion a very great contribution to our cryptanalytic operations has been made by Mr. A. J. Denniston, head of the Diplomatic Division of GC & CS and by Mr. E. W. Travis, head of the Services Division of GC & CS. It would be a nice gesture testifying to our appreciation if Medal for Merit awards could be obtained for the latter two, and a rank in the Legion of Merit for Colonel Tiltman.

b. The late Mr. A. H. Reiber's contribution toward the development of the various equipments mentioned above, in which he was ably assisted by Mr. W. Zenner, has been of sufficient importance to warrant recommendations for Medal of Merit awards on their behalf.

c. In addition to the foregoing I attach an R & W Sheet dealing with the matter of an award for Mr. L. A. Thompson of Acme Newspictures, Inc., on which Captain Prehn has prepared some data.

d. There is also attached an R & W Sheet from Colonel Collins to me, dealing with Mr. Reiber's case and also with that of Mr. Frank A. Cowan, of the A.T. & T. Company.

e. Drafts of the recommendations submitted by Colonel Harold Doud are returned herewith, together with those submitted by the Chiefs of A, B, C, E, and F Branches.

William F. Friedman
Director of Communications
Research

Attchd:

1. R & W re L.A. Thompson /s/ Capt. Prehn
2. R & W re Mr. Cowan and Mr. Reiber
3. 4 ltrs. /s/ Col. Doud
4. Memo re "A" Br. /s/ Sheetz
5. Memo re "B" Br. /s/ Cook
6. R & W re "C" Br. /s/ Allsopp
7. Memo re "E" Br. /s/ Brown
8. R & W re "F" Br. /s/ Rosen

~~SECRET~~