

AFSA-00/dk
Serial: 000241~~TOP SECRET~~~~TOP SECRET~~

4 NOV 1950

MEMORANDUM FOR DIRECTOR, COMMUNICATIONS-ELECTRONICS:

SUBJECT: Reports of the United Kingdom-United States Communication Security Conference.

Enclosure: One copy of subject reports.

1. As per our recent conversation, I am forwarding herewith for your information, an advance copy of subject reports, which are being submitted to AFSAC for consideration and approval prior to submission to the Joint Chiefs of Staff via the Director, Communications-Electronics.

2. The reports consist of -

Enclosure (A) Report on the Replacement of the CCM.
Enclosure (B) Report setting forth the results of the exploratory exchange of information on certain cryptographic developments.

3. The subject conference proved to be a most successful one from both the U.S. and British standpoints, and I feel that a good foundation for future effective collaboration in the cryptographic field has been established.

EARL E. STONE
Rear Admiral, U.S. Navy
Director, Armed Forces Security Agency

Copy to:

AFSA-12

AFSA-00

AFSA-123

RADM Earl E. Stone/dk/4 Nov 50
AFSA-00, Ext. 528

~~TOP SECRET~~

~~TOP SECRET~~

FIN

~~TOP SECRET~~BRITISH-UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FINAL MEETING OF THE PLENARY COMMITTEE

The Final Meeting of the Plenary Committee of the British-United States Communications Security Conference was held at 1515 on 27 October 1950 in Room 1212, U.S. Navy Security Station, Washington, D.C.

REPRESENTATIVES PRESENTUNITED STATES

Mr. W.F. Friedman, Chairman
 Rear Admiral Earl E. Stone, USN
 Captain L.F. Safford, USN
 Captain H.O. Hansen, USN
 Captain J.S. Harper, USN
 Colonel R.C. Sears, USAF
 Colonel John C. Arrowsmith, USA
 Colonel Roy H. Lynn, USAF
 Colonel Orville Laird, USAF
 Lt. Colonel R.H. Horton, USA
 Lt. Colonel Kelse G. Clow, USA
 Commander G.W. Linn, USN
 Dr. A. Sinkov

UNITED KINGDOM

Mr. T.R.W. Burton Miller
 Mr. J.M.G. Pollard
 Brigadier J.H. Tiltman
 Commander J.R.G. Trechman, R.N.

SECRETARIAT

LT J.W. Pearson, USN
 Mr. H.D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

ADMIRAL STONE called the meeting to order. He said that he had received a note from Brigadier General McClelland in which he expressed his regret at not being able to attend the closing Plenary Session. He explained that official business had required General McClelland's presence in San Antonio, Texas, and the General had asked that his apologies be conveyed to all concerned and that his best wishes be extended to the British delegates.

ADMIRAL STONE then stated that the Session had before it final versions of two reports to be approved for forwarding to the respective British and U.S. Chiefs of Staff. He suggested that, unless there was further comment, the final versions of the reports be signed at that time.

ADMIRAL STONE and MR. MILLER proceeded with the signing, and exchange of copies, of the final reports.

ADMIRAL STONE said that he wished to express his appreciation for the work which had been accomplished, adding his feeling that a firm groundwork for future operations in the Communications Security field had been laid. He expressed his opinion that the conference had been most worthwhile, and said that he thought much good would come of it.

ADMIRAL STONE asked Mr. Miller if he had any comments he wished to make.

MR. MILLER responded with the following remarks:

"Thank you very much for your remarks about the Conference. May I also thank you on behalf of the other members of the British team who were not able to be here for the close of this Conference. As you may know, Capt. Cairns is already in England, and the machinery is practically set for the return of the others of our group. Mr. Jolley is waiting in New York, and Lt. Col. Ham-Collins is in Canada, from whence he will return to New York and fly home from there. So far as the Conference is concerned, I would thoroughly endorse your remarks that the Conference has been an outstanding success. It has been a landmark in this particular art. It is a landmark in terms of its success, and in that it has covered a far wider field than has ever been covered before, and I feel that all items were discussed with great frankness and freedom. I would like to thank all the members of your team on every level for their cooperation and personal kindness; we have thoroughly enjoyed our part in the discussions and also the lighter vein which has been introduced from time to time. In every discussion we have learned a great deal, and we will go back home with a lot of information which will be valuable to us, and I hope that we have left behind something which will be of value to you.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

"There is one aspect which has been brought very firmly home to me. In 1941 we stood in dire need of a combined cypher machine. The problem was examined and it was found that the U.S. and British cypher machines were irreconcilable, and it was by luck and ingenuity, rather than by forethought, that the CCM which we have at this moment was devised and was used almost throughout the war. It was, however, a machine which was less secure than the British and U.S. National Machines. Having made those remarks, which might seem disparaging, I would like to remark that that machine without a doubt was our salvation. In 1950, we have had the British and U.S. Communications Security Conferences, and once more we find that in respect to some of the items discussed, development by the British and U.S. has reached a point where reconciliation of the machines as they stand is going to be extremely difficult. The lesson I have learned is that if we are going to achieve satisfactory Combined Communications, we should have regular and frequent discussions on these matters before designs are frozen and modification becomes impossible.

"I think I have nothing else to say other than to thank you for your personal kindness. We look forward to having you join us in London next year, and we hope that we can reciprocate in some way the kindness which we have received at your hands."

ADMIRAL STONE thanked Mr. Miller for his remarks, and said that he would like to express his appreciation to all members of the British team. He expressed regret that the entire British delegation could not be present at this final Session, and asked that Mr. Miller convey to them the best wishes of the U.S. delegates.

ADMIRAL STONE then asked for any further comments.

There were none, and the Meeting was declared adjourned at 1535.

~~TOP SECRET~~

~~SECRET~~

BRUSA COMSEC CONFERENCE

Plenary Committee

AGENDA

**For the closing meeting to be held at 1500, 27 October 1950,
Room 1212, NAVSECSTA**

- 1. Approval of the Report to the U.S. and British Joint Chiefs of Staff by the BRUSA Communication Security Conference.**
- 2. Closing remarks by Mr. Miller.**
- 3. Closing remarks by Admiral Stone.**

~~SECRET~~

~~SECRET~~

18 October 1950

SUBJECT: BHUSA Communication Security Conference**TO: Individuals listed in paragraph 2.**

1. The closing Combined Meeting of the BHUSA Communication Security Conference will be held in Room 1212, Navy Security Station, at 1500 on Friday, 27 October 1950.

2. The following United States personnel are invited to attend this meeting.

PLENARY COMMITTEE

Rear Admiral Earl E. Stone, USN
Major General H. M. McClelland, USAF +
Colonel S. P. Collins, USA
Captain J. N. Wenger, USN
Colonel R. H. Lynn, USAF

SERVICE CRYPTOLOGIC AGENCIES

Brigadier General William W. Gillmore, USA +
Captain L. S. Howeth, USN
Colonel Orville J. Laird, USAF x

EXECUTIVE COMMITTEE

Mr. W. F. Friedman
Captain H. O. Hansen, USN
Captain J. S. Harper, USN
Colonel R. C. Sears, USAF
Lieutenant Colonel R. H. Horton, USA

SECRETARIAT

Lieutenant J. W. Pearson, USN
Mr. H. D. Jones

CHAIRMAN, SUBCOMMITTEE A

Captain L. F. Safford, USN

CHAIRMAN, SUBCOMMITTEE B

Dr. A. Sinkov

William F. Friedman

WILLIAM F. FRIEDMAN
Chairman, Executive Committee

~~SECRET~~

~~SECRET~~

12 October 1950

SUBJECT: BRUSA Communication Security Conference

TO: Mr. W. F. Friedman

1. The Combined Executive Committee Meeting and the closing Combined Plenary Session of the BRUSA Communication Security Conference scheduled for 1000 and 1100 hours, respectively, Friday, 13 October 1950, have been postponed until sometime after 23 October 1950.

2. Information regarding a new time and date will be furnished as soon as available.



WILLIAM F. FRIEDMAN,
Chairman, Executive Committee

~~SECRET~~

~~SECRET~~

5 October 1950

SUBJECT: BRUSA Communication Security Conference.

TO: Individuals listed in paragraph 2.

1. The closing Combined Meeting of the BRUSA Communication Security Conference will be held in Room 1212, Navy Security Station, at 1100 on Friday, 13 October 1950.

2. The following United States personnel are invited to attend this meeting.

PLENARY COMMITTEE

Rear Admiral Earl E. Stone, USN
Major General H. M. McClelland, USAF
Colonel S. P. Collins, USA
Captain J. N. Wenger, USN
Colonel R. E. Lynn, USAF

SERVICE CRYPTOLOGIC AGENCIES

Brigadier General William N. Gillmore, USA
Captain L. S. Howeth, USN
Colonel Orville J. Laird, USAF

EXECUTIVE COMMITTEE

Mr. W. F. Friedman
Captain H. O. Hansen, USN
Captain J. S. Harper, USN
Colonel R. C. Sears, USAF
Lieutenant Colonel R. H. Horton, USA

SECRETARIAT

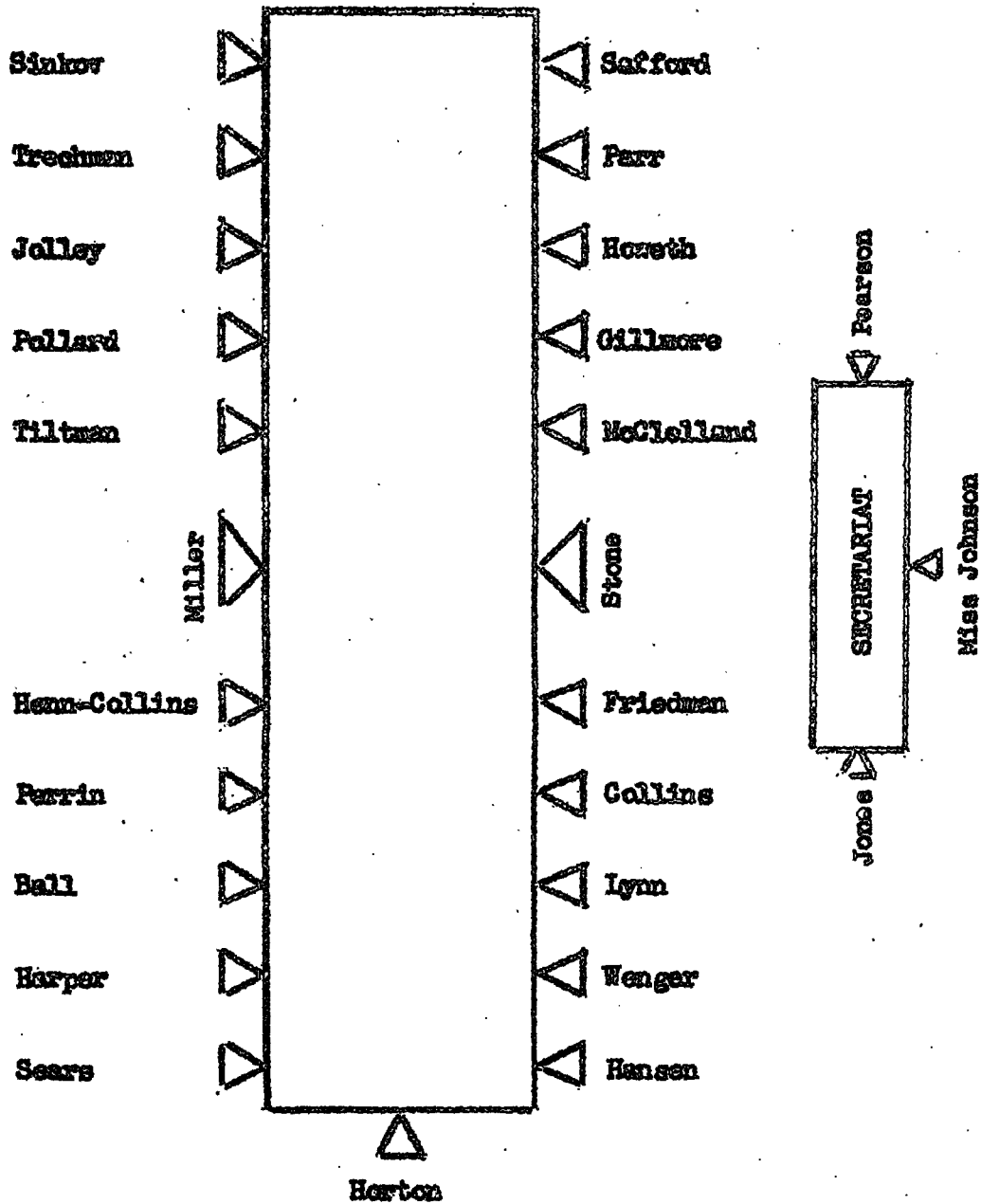
Lieutenant J. W. Pearson, USN
Mr. H. D. Jones

CHAIRMAN, SUBCOMMITTEE A
Captain L. F. Safford, USN

CHAIRMAN, SUBCOMMITTEE B
Dr. A. Sinkov

William F. Friedman
WILLIAM F. FRIEDMAN,
Chairman, Executive Committee

~~SECRET~~



Seating arrangement for the Plenary Session, BRUSA Communication Security Conference, scheduled for 1100 hours, Friday, 13 October 1950.

~~SECRET~~*Mr. Friedman*
OOTBRUSA COMSEC CONFERENCE

Schedule of Meetings for the Week Beginning 9 October 1950

Monday, 9 October 1950.

- 1000 Meeting of Subcommittee A.
- 1330 Continue meeting of Subcommittee A.

Tuesday, 10 October 1950.

- 1000 Completion of discussions and drafting of reports by Subcommittee A.
- 1330 Completion of discussions and drafting of reports by Subcommittee B.

Wednesday, 11 October 1950.

- 0800 Typing of reports.
- 1400 Executive Committee meeting to consider the reports of Subcommittees A and B. Meeting in Room 1212, Navy Security Station.

Thursday, 12 October 1950

- 1000 Executive Committee meeting, if required. Meeting in Room 1212, Navy Security Station.
- 1300 Retyping of final reports.

Friday, 13 October 1950

- 1000 Executive Committee meeting to approve final reports, Room 1212, Navy Security Station.
- 1100 Plenary Committee meeting, Room 1212, Navy Security Station.

~~SECRET~~

~~SECRET~~

5 October 1950

SUBJECT: BRUSA Communication Security Conference.

TO: Individuals listed in paragraph 2.

1. The closing Combined Meeting of the BRUSA Communication Security Conference will be held in Room 1212, Navy Security Station, at 1100 on Friday, 13 October 1950.

2. The following United States personnel are invited to attend this meeting.

PLENARY COMMITTEE

Rear Admiral Earl E. Stone, USN
Major General H. M. McClelland, USAF
Colonel S. P. Collins, USA
Captain J. N. Wenger, USN
Colonel R. H. Lynn, USAF

SERVICE CRYPTOLOGIC AGENCIES

Brigadier General William N. Gillmore, USA
Captain L. S. Howeth, USN
Colonel Orville J. Laird, USAF

EXECUTIVE COMMITTEE

Mr. W. F. Friedman
Captain H. O. Hansen, USN
Captain J. S. Harper, USN
Colonel R. C. Sears, USAF
Lieutenant Colonel R. H. Horton, USA

SECRETARIAT

Lieutenant J. W. Pearson, USN
Mr. H. D. Jones

CHAIRMAN, SUBCOMMITTEE A
Captain L. F. Safford, USN

CHAIRMAN, SUBCOMMITTEE B
Dr. A. Sinkov

William F. Friedman
WILLIAM F. FRIEDMAN,
Chairman, Executive Committee

~~SECRET~~

~~TOP SECRET~~

27 September 1950

MEMORANDUM FOR THE MEMBERS OF THE PLENARY COMMITTEE:

Subject: Tentative Minutes of the First Meeting.

1. The subject minutes are forwarded herewith for your consideration.

2. Please advise the Secretariat, located in Room 211, Building 19, U. S. Navy Security Station, telephone extension -- 354, of your comments and/or concurrence.



J. W. PEARSON
H. D. JONES
Secretariat

~~TOP SECRET~~

~~TOP SECRET~~BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FIRST MEETING OF THE PLENARY COMMITTEE

The First Meeting of the Plenary Committee of the British - United States Communications Security Conference was held at 1430 on 21 September 1950 in Room 1212, U. S. Navy Communication Station, Washington, D. C.

Representatives PresentUnited StatesUnited Kingdom

✓ Rear Admiral Earl E. Stone, USN
 Major General H. M. McClelland, USAF
 Brigadier General W. N. Gillmore, USA
 Colonel R. H. Lynn, USAF
 Captain L. S. Howeth, USN
 Colonel O. J. Laird, USAF
 ✓ Colonel S. P. Collins, USA
 Captain L. F. Safford, USN
 Captain J. N. Wenger, USN
 Captain J. S. Harper, USN
 Colonel R. C. Sears, USAF
 Captain H. O. Hansen, USN
 Lt. Col. R. H. Horton, USA
 Mr. W. F. Friedman
 Dr. A. Sinkov

Mr. T.R.W. Burton Miller
 Captain, the Earl Cairns, R.N.
 Mr. Kenneth Perrin
 Mr. J.M.G. Pollard
 Lt. Col. C. A. Henn-Collins
 Mr. E. H. Jolley
 Brigadier J. H. Tiltman
 Group Captain Benjamin Ball, RAF
 Commander J.R.G. Trechman, R. N.

Secretariat

Lieutenant J. W. Pearson, U.S.N.
 Mr. H. D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~

ADMIRAL STONE opened the First Plenary Session of the British - United States Communications Security Conference by welcoming the British Delegation on behalf of the U. S. Representatives. Stating that this Conference was another link in the chain of friendly U. S. - British relations, Admiral Stone emphasized the advantages of collaboration in the vitally important related fields of Communications Intelligence and Communications Security, and remarked that this Conference represented a further step in British-U.S. collaboration in that it was concerned with Communication Security developments of a rather wide scope. He continued by stressing the importance of combined communications security, and stated that all concerned were striving to assure the maintenance of adequate security in combined communications on various levels. He added that it was his hope that collaboration would do more than to assure the maintenance of adequate security, explaining that in the reciprocal exchange of cryptographic information, the United States Technical Experts, although feeling that they had much to offer, knew that they would gain much useful technical information from the exchange with their British colleagues, and further that such information should have beneficial effects on the security of purely U.S. Communications, and that reciprocally, it was hoped that whatever information U. S. Technicians could provide, would prove beneficial to the security of purely British Communications.

Concluding his remarks by expressing the hope that the visit of the British Delegation to the United States would be a pleasant one, Admiral Stone invited the members of the Delegation to call upon him for any personal assistance that he might be able to render. He then invited Mr. Burton Miller, Head of the British Delegation, to address the Conference.

MR. MILLER, speaking on behalf of the British Delegation, thanked Admiral Stone for his words of welcome, stating that they had been looking forward to their visit, and to getting on with the discussion of the items on the agenda. He remarked that discussions on some of the items had been held before, and that they had proved very profitable. He stated that one or two aspects had presented stumbling blocks, which had been satisfactorily removed, and therefore he saw no reason why decisions could not be reached at this time on which both parties could build and forge ahead. He pointed out that notwithstanding the name "Initial Exploratory Conference", he felt that decisions could be reached on certain items which would be of mutual benefit to both parties, but that much benefit could be gained from exploratory discussions of other items on which firm decisions could not be reached at this time. Stating his desire to make the maximum contribution during the deliberations and discussions to follow, Mr. Miller concluded his remarks.

~~TOP SECRET~~

~~TOP SECRET~~

ADMIRAL STONE thanked Mr. Miller, and invited General McClelland, Director, Communications-Electronics and Chairman of the Joint Communications-Electronics Committee, to address the Conference.

GENERAL McCLELLAND, extending additional words of welcome to the British Delegation, recalled that since the establishment of his office, approximately one year ago, he had noted increasing collaboration between the U. K. and the U. S., particularly with regard to the Military Services of the two countries. In explaining the functions of his office, General McClelland stated that it had been established under the Joint Chiefs of Staff to provide overall coordination among the communications-electronics activities of the three Services, and that control and supervision was vested in the Joint Communications-Electronics Committee which operated similarly to BJCB. He continued by saying that the Joint Communications-Electronics Committee was a completely integrated organization, having two Colonels from the Army, two Captains from the Navy, and three Colonels from the Air Force; he emphasized the fact that his own position was completely neutral.

GENERAL McCLELLAND pointed out that the Director, Communications-Electronics also served as the Chairman of the Joint Communications-Electronics Committee, the Chairmanship being rotated among the three Services every two years. He remarked that a great deal had been learned from the British during the War concerning Committee Government, particularly the principle of unanimous decisions, and that while he had the authority to resolve a split vote, it had never been necessary for him to do so. He concluded his remarks by pointing out that the Joint Communications-Electronics Committee had a responsibility to the Armed Forces Security Agency in that it was charged with providing communications for that Agency's communications intelligence activities.

ADMIRAL STONE thanked General McClelland, and stated that the Conference had progressed to a point at which he thought it would be appropriate to select a Conference Chairman. On behalf of the United States Delegation, Admiral Stone stated that he was pleased to offer the Chairmanship to the British Delegation.

MR. MILLER, thanking Admiral Stone for his offer, commented that he was not sure if it would not be advantageous to have an American Chairman.

ADMIRAL STONE replied that the American Delegation would be very happy to have the British provide the Chairman, particularly in the person of Mr. Miller.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER stated that he was happy to accept the Chairmanship.

Before turning the Chair over to Mr. Miller, Admiral STONE said that there were several matters that needed to be covered; he requested Mr. Friedman to present a statement setting forth information that would be useful as background for the Conference.

✓ MR. FRIEDMAN stated that he thought it necessary to invite the delegates' attention to the fact that there are in existence certain agreements between the United Kingdom of Great Britain and Northern Ireland and the United States, and between the U. K. Chiefs of Staff and the U. S. Chiefs of Staff with regard to (1) security measures for the protection of classified military information disclosed by or exchanged between the two governments, and (2) arrangements for the protection of the rights of inventors of equipments disclosed by or exchanged between the two governments.

UK-U.S. MR. FRIEDMAN then read the following two articles from the current agreement regarding mutual defense assistance which entered into force on 27 January 1950:

"Article V

"1. Each contracting Government will take such security measures as may be agreed in each case between the two contracting Governments in order to prevent the disclosure or compromise of any classified military articles, services, or information furnished by the other contracting Government pursuant to this Agreement.

"2. Each contracting Government will take appropriate measures consistent with security to keep the public informed of activities under this Agreement.

"Article VI

"1. The two contracting Governments will negotiate appropriate arrangements between them respecting responsibility for claims for the use or infringement of inventions covered by patents or patent applications, trademarks, or copy rights, or other similar claims arising from the use of devices, processes, or technological information in connection with equipment, materials, or services furnished pursuant to this Agreement, or furnished in the interests of production undertaken by agreement between the two contracting Governments in implementation of the pledges of self-help and mutual aid contained in the North Atlantic Treaty."

~~TOP SECRET~~

~~TOP SECRET~~

Continuing his remarks, Mr. FRIEDMAN pointed out that it was assumed that this Conference would take cognizance of the foregoing articles in the U. K. - U. S. agreement, and that the representatives of the respective Governments would govern themselves accordingly. He emphasized that in order to be on the safe side, it was to be understood that all information disclosed during the Conference would be regarded as classified information, regardless of whether such classification is in the military sense or in the sense of "Confidential" as used in the processing of patent applications through the Patent Offices of either or both governments.

MR. FRIEDMAN concluded his remarks by stating that Admiral Stone had designated Lieutenant Pearson as his (Admiral Stone's) representative to receive requests for any written technical information or drawings which might be desired by the British Mission, and that such data as might be available would be transmitted from Admiral Stone's office to the Head of the British Mission.

ADMIRAL STONE said that he would turn the Chairmanship over to Mr. Miller at this time, stating that he would be pleased to assist the Chairman in any way possible.

MR. MILLER replied that upon reflection, he felt that it would be better if Admiral Stone assumed the Chair.

ADMIRAL STONE stated that he would be pleased, and if it were agreeable, he would take the Chair. He suggested that it might be well at this time to review the Conference Agenda, explaining that it was composed of two parts: (1) Replacement for the Combined Cipher Machine, and (2) Exploratory. He pointed out to Mr. Miller that he had altered the order of the items as a result of their discussions on Wednesday, 20 September 1950.

MR. MILLER replied that the order of items on the Agenda was agreeable to him.

ADMIRAL STONE continued by saying that as had already been indicated, U. S. Authorities hoped to come to some specific understanding on the first item on the Agenda, and that he had designated Captain Safford, U.S.N., who had had a great deal of experience with the seven rotor BCM, to be his representative in disclosing and discussing that machine. He suggested that if it were agreeable to the British Delegation, he would set 0930, 22 September 1950, as the time for showing the seven rotor machine in Room 319 of Building 17, stating that the U. S. Delegation were prepared to spend the remainder of the morning discussing the machine, and at the pleasure of the British Delegation, the discussions would be resumed in the afternoon. He inquired of Mr. Miller if the foregoing proposals were agreeable.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER replied in the affirmative.

ADMIRAL STONE remarked that it might be possible for the Conference to proceed on Monday of next week with the exploratory discussions, pointing out that U. S. Representatives had prepared a suggested form, Enclosure A to the Agenda, which showed the scope of the discussions. He inquired if the Agenda with Enclosure A were generally satisfactory to the British Delegation.

MR. MILLER replied that the Agenda, with Enclosure, was satisfactory, stating that they had already had an opportunity to study some of the problems. He explained that one exhibit and quite a number of papers were supposed to have come over with the British Delegation on the Queen Elizabeth, but present indications were that they had not been aboard, however, he added, he had taken steps to have them dispatched as soon as practicable.

ADMIRAL STONE stated his appreciation of the situation, and added that perhaps it would permit the British Delegation to remain in Washington longer than had been anticipated. Turning to the next item of the Plenary Agenda, he proposed that the matter of Committee Structure be considered next. He observed that a paper, indicating the U. S. representation on the Plenary Committee, Executive Committee, and Sub-Committees A and B, had been distributed, and suggested that it might be advisable to ascertain the names of the British representatives for the Executive and Sub-Committees at this time. With regard to the selection of Chairmen for the several Committees, Admiral Stone suggested that the British Delegation designate the Chairman for the Executive Committee and Sub-Committee B, but stated his preference for retaining Captain Safford as Chairman of Sub-Committee A, in view of the fact that the United States was the disclosing authority.

MR. MILLER indicated his agreement to Admiral Stone's suggestion, stating that his delegation was so small, they would work as a team on most of the items. He stated his preference for restricting British membership on the Committees to the Delegation itself, reserving the privilege of calling in various British residents of Washington from time to time.

Indicating his agreement with Mr. Miller's remarks, Admiral STONE said that he assumed that the full British Delegation would be a part of the Plenary Committee, unless Mr. Miller would prefer some other arrangement.

MR. MILLER replied in the affirmative.

~~TOP SECRET~~

~~TOP SECRET~~

ADMIRAL STONE announced that there would be a meeting of the Executive Committee immediately following the Plenary Meeting at which time the times and places of future meetings could be arranged. Turning to another subject, he recalled that the matter of standardization of rotors had already been mentioned in a paper which had been forwarded to the British, and that U. S. Authorities were of the opinion that the interchange of rotors on whatever machine is agreed upon for combined use was of utmost importance; he proposed therefore, that the subject of standardization of rotors be included in the discussions on the replacement of the Combined Cipher Machine.

MR. MILLER agreed to the proposal.

ADMIRAL STONE then requested Mr. Miller to act as, or designate, the Chairman of the Executive Committee, at least on a temporary basis.

MR. MILLER replied that he himself would assume the Chairmanship of the Executive Committee, at least for the Meeting today.

ADMIRAL STONE inquired whether there were any further comments to be made at this time.

CAPTAIN HOWETH stated that he would like to take this opportunity of welcoming some of his old friends to Washington.

ADMIRAL STONE introduced the members of the U. S. Delegation, and welcomed Group Captain Ball and Commander Trechman to the meeting. He stated that Mr. Friedman, Colonel Collins, and Colonel Lynn would be his representatives at the Meeting of the Executive Committee to follow.

The meeting adjourned at 1456.

~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A67163

Office Memorandum • UNITED STATES GOVERNMENT

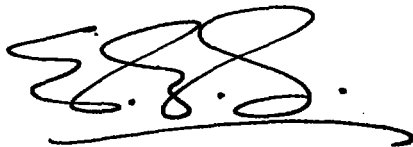
TO : AFSA-14

DATE: 24 August 1950

FROM : DIRAFSA

SUBJECT: U.S. - British Conference on the Exchange of Cryptographic Principles
on a Reciprocal Basis (AFSAC: 63/1)

Please draft appropriate opening remarks for my use at subject conference.



EARL E. STONE
Rear Admiral, U.S. Navy
Director, Armed Forces Security Agency

~~TOP SECRET~~

~~SECRET~~

D R A F T

It is with a great deal of pleasure that I welcome the British Delegation from GCHQ to the United States and to the Armed Forces Security Agency. I am sure you are all aware of this new Agency, which was created a little over a year ago and has brought about a further integration of the cryptologic operations conducted by and within the Armed Forces of the United States. In using the word cryptologic I mean to indicate that AFSA is now in a position to deal with the whole coin, one side of which represents the communication intelligence activities, the other, the communication security activities of the Armed Forces of the United States. AFSA is, in fact, now an organization rather similar to GCHQ, which we, on this side of the water, have always admired for its great accomplishments and successes throughout the years of our association.

British-U.S. collaboration in the communication intelligence field was very close during World War II, so close, in fact, that its beneficial

~~SECRET~~

~~SECRET~~

results represented a major contribution in the successful outcome of that war. The details of that story are pretty well known to all of us here today and need not be elaborated on at this time, except to say that the close war-time collaboration in that field has been extended to our present so-called peace-time.

Also during World War II, there was British-U.S. collaboration in the communication security field, a no less important activity, and in some respects even more important than the COMINT, or, as our British friends say, the SIGINT field. The collaboration was not as complete, perhaps, since it involved for the most part only the security of highest-level Combined communications. But, again, success greeted our Combined efforts, even though it might have been noted in less spectacular fashion. The present Conference represents a further step in British-U.S. collaboration in the field of cryptology, for it is devoted to communication security matters of fairly wide scope. Not only will there be discussions on Combined Communications of the

~~SECRET~~

~~SECRET~~

highest level, and specifically on the CGM, but also we expect to discuss Combined Communications of all levels and to go to a certain extent into the general field of cryptographic principles to include those underlying other types of literal cipher machines, as well as ciphony and cifax devices. Not only are the U.S. representatives prepared to discuss these subjects but also they will be glad to demonstrate certain devices in the form of final equipments, or engineering models, or breadboard models of certain new equipments.

In the U. S. Armed Forces the question has often arisen: which is the more important of the two closely associated segments of cryptologic science -- communication intelligence or communication security? Workers engaged in the former naturally regard their field as paramount; those engaged in the latter regard their own as being first in importance, and no amount of argument will convince them otherwise. However, if backed into a corner, the COMINT specialists will admit that should matters ever come to so serious a crisis that a decision would have to be made to abandon one or the other activity, they feel sure of what the

~~SECRET~~ -

~~SECRET~~

answer would be, and they would reluctantly fold up their tents. I have no doubt as to where the members of the British Delegation stand on that question. I will admit that in my position it is sometimes difficult to make a decision based on the relative importance of the two, but in the present instance I feel that we are all of one mind. On the safety of our communications lies not only the safety of our COMINT activities, but also the security of all our strategic and tactical military, naval, and air plans and operations, the safety of our own Armed Forces, and hence the security of our Governments. We hope never to be in a position where, in forthright parlance, "telegraphing our punches" results in the loss of a life, a battle, a campaign, or a war. Of course, we in the cryptologic service do not have the sole responsibility in that regard, because the commanders of forces afield, afloat, and in the air are the actual users of the equipment we conceive, design, and provide. Theirs is the responsibility to see that the equipment is used properly and efficaciously. But we cannot dodge the responsibility of providing adequate security together

~~SECRET~~ 4 -

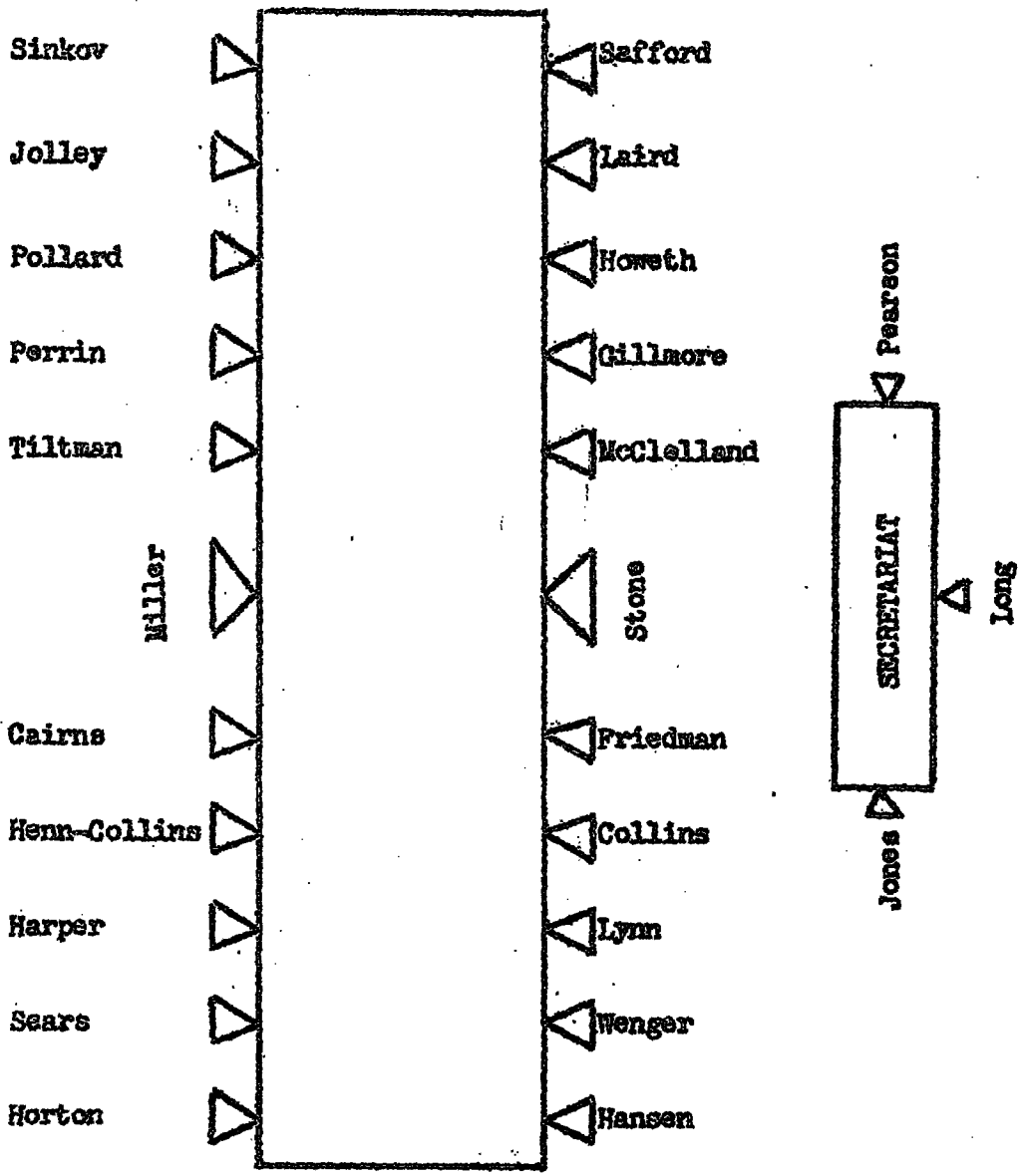
~~SECRET~~

with maximum operability. When we have done that, then and only then can our consciences be clear as regards our responsibilities in the matter of communication security.

The present Conference is a preliminary step in paving the way toward achieving adequate security in Combined Communications of various levels. But I hope that it will do more than that. For in the reciprocal exchange of cryptographic principles the United States technical experts, although they feel that they have much to offer, feel equally sure that they can and will gain much useful technical information from their British opposite numbers in the discussions. Such information will have beneficial effects on the security of purely U.S. communications and, reciprocally, we hope that such information as U. S. technicians can provide will prove beneficial to the security of purely British communications. Thus, we will all benefit: U. S. communications, British communications, and Combined communications, will all be improved.

Before proceeding further with Conference business, I am sure we would all like to hear from Mr. Miller, the Chief of the British Delegation.

~~SECRET~~



~~SECRET~~

18 September 1950

SUBJECT: BRUSA Communications Security Conference

TO: Individuals listed in paragraph 2.

1. The opening Combined Meeting of the BRUSA Communication Security Security Conference will be held in Room 1212, Naval Communication Station, at 1430 on Thursday, 21 September 1950.

2. The following United States personnel have been invited to attend this Meeting:

Rear Admiral Earl E. Stone, USN	}	Plenary Committee
Major General H. M. McClelland, USAF		
Colonel S. P. Collins, USA		
Captain J. N. Wenger, USN		
Colonel R. H. Lynn, USAF		

Brigadier General William N. Gillmore, USA	}	Service Cryptologic Agencies
Captain L. S. Howeth, USN		
Colonel Orville J. Laird, USAF		

Mr. W. F. Friedman	}	Executive Committee
Captain H. O. Hansen, USN		
Captain J. S. Harper, USN		
Colonel R. C. Sears, USAF		
Lieutenant Colonel R. H. Horton, USA		

Lieutenant J. W. Pearson, USN	}	Secretariat
Mr. H. D. Jones		

Captain L. F. Safford, USN, Chairman, Subcommittee A
 Dr. A. Sinkov, Chairman, Subcommittee B

W. F. Friedman
 W. F. FRIEDMAN
 Chairman, Executive Committee

~~TOP SECRET~~~~TOP SECRET~~BRUSA COMSEC CONFERENCEAGENDA FOR U. S. - BRITISH CONFERENCE ON THE EXCHANGE OF
CRYPTOGRAPHIC PRINCIPLES

- a. Special Purpose Teleprinter Systems for the Exchange of Intelligence Material.
- b. Low Echelon (Minor War Vessels) Telegraphic Systems.
- c. Merchant Ship Telegraphic Systems.
- d. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.
- e. Voice Security Systems for Tactical Purposes.

It is proposed that each of the above types of systems be discussed according to the schedule set forth in Enclosure A hereto.

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

Enclosure A

I. Desirable Characteristics.

A. General

1. Objective
2. Type or level of Employment

B. Operational Characteristics

1. Security
 - a. Cryptosecurity
 - b. Radiation Security
 - c. Transmission Security
2. Functional Requirements
3. Radio Interference
4. Power Requirements
5. Special Requirements

C. Physical Characteristics

1. Weight and Volume Factors
2. Operation, Transportation, Packaging and Storage Requirements
3. Destruction Requirements

D. Operation and Maintenance Characteristics of Equipment

E. Comint Implications with Respect to Consequences of Capture of Equipment

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

Enclosure A (continued)

- II. Present Equipment - U.S.
 - A. Demonstration or Description
 - B. Discussion concerning Adequacy According to I (Interim, Long-range, Emergency)
- III. Present Equipment - U.K.
 - A. Description or Model Demonstration
 - B. Discussion concerning Adequacy According to I
- IV. Equipment under Development - U.S.
 - A. Description or Model Demonstration
 - B. Adequacy according to I
 - C. Present Status
 - D. Plans
- V. Equipment under Development - U.K.
 - A. Description or Model Demonstration
 - B. Adequacy according to I
 - C. Present Status
 - D. Plans

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~

FINAL

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FIFTH MEETING OF THE EXECUTIVE COMMITTEE

The Fifth Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1400 on 27 October 1950 in Room 1212, U. S. Navy Security Station, Washington, D. C.

Representatives PresentUnited States

Mr. W. F. Friedman, Chairman
Rear Admiral Earl E. Stone, U.S.N.
Captain L. F. Safford, U.S.N.
Captain H. O. Hansen, U.S.N.
Captain J. S. Harper, U.S.N.
Colonel R. C. Sears, U.S.A.F.
Lt. Colonel R. H. Horton, U.S.A.
Lt. Colonel Kelso G. Clow, U.S.A.
Dr. A. Sinkov

United Kingdom

Mr. T.R.W. Burton Miller
Mr. J.M.G. Pollard
Brigadier J. H. Tiltman
Commander J.R.G. Trechman, R.N.

Exec
Comm.Secretariat

Lieutenant J. W. Pearson, U.S.N.
Mr. H. D. Jones
Miss Catherine M. Johnson

~~TOP SECRET~~

ITEM 1. APPROVAL OF THE MINUTES OF THE FOURTH MEETING.

MR. FRIEDMAN stated that the minutes of the Fourth Meeting were still in preparation and were not available for consideration. He explained that it was realized that this would be the case, however, it was believed advisable to include this item on the agenda for purpose of record.

ITEM 2. APPROVAL OF THE THIRD REPORT OF SUB-COMMITTEE A.

MR. FRIEDMAN introduced this item for consideration, stating that the problem before the Committee was one of checking to see that the revisions agreed to at the last meeting had been recorded properly in the final paper which was now before the Committee. He asked if the members had had an opportunity to study this paper.

MR. MILLER replied in the affirmative and said that the final version met with his approval.

CAPTAIN SAFFORD expressed his satisfaction with the final version.

The Committee agreed to approve the Third Report of Sub-Committee A, as revised at the Fourth Meeting of the Executive Committee.

ITEM 3. APPROVAL OF THE SECOND REPORT OF SUB-COMMITTEE B.

MR. FRIEDMAN asked for comments on the final version of this report, which included changes agreed to at the Fourth Meeting.

DR. SINKOV said that he had read the final paper carefully to see that the agreed changes had been made. He added that he was entirely satisfied with the paper.

MR. MILLER said that he, also, was satisfied with the final version.

The Committee agreed to approve the Second Report of Sub-Committee B, as revised at the Fourth Meeting of the Executive Committee.

~~TOP SECRET~~

ITEM 4. APPROVAL OF THE REPORTS TO THE U.S. JOINT CHIEFS OF STAFF AND THE BRITISH JOINT CHIEFS OF STAFF BY THE BRUSA COMMUNICATIONS SECURITY CONFERENCE.

MR. FRIEDMAN introduced the final item for consideration and suggested that the two final reports be considered paragraph by paragraph. This suggestion was accepted and the members proceeded to consider the first of two reports:

Report on Replacement of the CCM

MR. FRIEDMAN read the basic report and Appendix A thereto.

After a brief discussion the Committee agreed to accept the report as written, except for the following changes on page 5 (in Appendix A):

Subparagraph (a). Change to read as follows:

"(a) That there should be issued 20 rotors to the set for each existing CCM in lieu of present number of 10. This is to become effective as soon as practicable, but shall not preclude issue of sets of 10 rotors in the interim. Key lists for 20-rotor sets should be so prepared that no rotor will ever be effective on two successive days, within the same key lists for each cryptochannel; so as to permit setting up two baskets for two successive days from a single set of 20 rotors thus obviating the need for duplicate sets of rotors."

The Secretariat arranged for the immediate publication of a new page 5, including the above change, copies of which were inserted in all copies of the subject report in lieu of the existing page 5.

Report on the Exploratory Conference

MR. FRIEDMAN then read, paragraph by paragraph, the report on the Exploratory Conference, and the members noted the previously-agreed changes which had been incorporated therein.

After brief discussion the members approved the final report without change.

MR. FRIEDMAN asked for any further comments on the reports just approved.

There were no further comments.

MR. FRIEDMAN then declared the Meeting adjourned (at 1510) and announced that there would be a brief recess before the final Meeting of the Plenary Committee.

~~TOP SECRET~~

~~SECRET~~

BRUSA COMSEC CONFERENCE

Executive Committee

AGENDA

For the Fifth meeting to be held at 1400, 27 October, 1950, in Room
1212 NAVSECSTA

1. Approval of Minutes of Fourth Meeting.
2. Approval of the Third Report of Subcommittee A.
3. Approval of the Second Report of Subcommittee B.
4. Approval of the Report to the U.S. and British Joint Chiefs of Staff by the BRUSA Communication Security Conference.

~~SECRET~~

~~TOP SECRET~~

FINAL

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FOURTH MEETING OF THE EXECUTIVE COMMITTEE

The Fourth Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1400 on Wednesday, 25 October 1950 in Room 1212, U. S. Navy Security Station, Washington, D. C.

Representatives PresentUnited StatesUnited Kingdom

Mr. H. F. Friedman, Chairman	Mr. T.R.W. Burton Miller
Rear Admiral Earl E. Stone, U.S.N.	Commander J.R.G. Trechman, R.N.
Captain L. F. Safford, U.S.N.	
Captain J. S. Harper, U.S.N.	
Colonel R. C. Sears, U.S.A.F.	
Captain H. O. Hansen, U.S.N.	
Lt. Col. K. G. Clow, U.S.A.	
Lt. Col. R. H. Horton, U.S.A.	
Dr. A. Sinkov	

Secretariat

Lieutenant J. W. Pearson, U.S.N.
Mr. H. D. Jones
Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~**ITEM 1. APPROVAL OF FINAL MINUTES OF THE THIRD EXECUTIVE COMMITTEE MEETING.**

Prior to consideration of the first item on the agenda, MR. FRIEDMAN welcomed Lieutenant Colonel Kelso G. Clow, Senior United States Liaison Officer, London, to the meeting.

MR. FRIEDMAN inquired if there were any comments or corrections to be made to the Final Minutes of the Third Meeting of the Executive Committee.

MR. MILLER replied that there were none from the British Delegation.

MR. FRIEDMAN, making reference to the first paragraph on page two, stated that the second line should have read in part "AFSA Office of Research and Development" to avoid confusion with the Research and Development Board of the Department of Defense.

The Executive Committee approved the Final Minutes of the Third Meeting as written.

In connection with the minutes under consideration, Mr. FRIEDMAN referred to the last paragraph on page six, and inquired of Mr. Miller whether he had received approval from GCHQ on the use of the code word "BRUTUS".

MR. MILLER replied that such approval had been obtained prior to the Third Meeting of the Executive Committee, and explained that he had inquired about the use of the codeword "AJAX", and had found that it was already in use, however, he added that he was agreeable to using "AJAX" in British-U.S. papers and correspondence as the designation for the 5-rotor CCM.

DR. SINKOV suggested that perhaps the U. S. could reconsider the matter, and find another name that did not conflict with British codeword terminology.

ADMIRAL STONE remarked that since the conflict was on the British side, and since Mr. Miller had indicated his willingness to go ahead and use the word, that he was of the opinion that it should then be used.

MR. MILLER commented that the signal he had received from GCHQ was not indicative as to what the word "AJAX" had been assigned to, but that he would like to make a reservation to the effect that he would be agreeable to the word's use, provided that it had not been assigned to some communications project, in which case a conflict could conceivably occur.

~~TOP SECRET~~

~~TOP SECRET~~**ITEM 3. CONSIDERATION OF THE SECOND REPORT OF SUBCOMMITTEE "B".**

MR. FRIEDMAN explained that Item 2 on the agenda would be deferred until Commander Trechman's arrival. He suggested that the Committee consider Item 3, and requested Dr. Sinkov's comments.

DR. SINKOV read the second report of Sub-Committee "B". He pointed out that the First Report had not been complete in that the appendices containing brief descriptions of the items discussed had not been attached. He explained that those appendices had now been added, along with the amendments agreed to at the Third Meeting.

After a brief discussion it was agreed that the following amendments would be made to the Second Report of Subcommittee "B":

1. Amend paragraph 1. to read as follows:

"1. Sub-Committee B has made an exchange of technical information concerning various cryptosystems falling in the general category of 'Special purpose teleprinter systems for the exchange of communications intelligence material.' The cryptosystems discussed are divided into the following groups:

	<u>NON-SYNCHRONOUS</u>		<u>SYNCHRONOUS</u>
	<u>ROTOR MAZE</u>	<u>KEY GENERATORS</u>	
U.S.	AFSAM-9	ASAM 2-1	AFSAM-9, if provided with synchronous features.
U.K.	- - - -	Rollick	5 U.C.O. (Secrettype)"

2. Amend paragraph 3a. to read as follows:

"3. a. We note that Rockex is presently being used for the exchange of communications intelligence material."

3. Amend paragraph 4b. to read as follows:

"4. b. Either machine is available in sufficient quantity to meet current requirements in the exchange of communications intelligence material."

~~TOP SECRET~~

~~TOP SECRET~~

4. 4. Amend paragraph 5 to read as follows:

"5. In the course of the discussions on equipments using one-time tapes, a brief description was given of British progress in key-tape production equipment. In view of the close association of such equipment with one-time systems, it is recommended that the subject of production equipment be added to the agenda of the next British-U.S. COMSEC conference."

Subject to the foregoing amendments, the Executive Committee approved the Second Report of Sub-Committee "B".

Commander Trechman joined the Committee at 1445.

~~TOP SECRET~~

ITEM 2. CONSIDERATION OF THE THIRD REPORT OF SUB-COMMITTEE "A".

MR. FRIEDMAN requested Captain Safford to read the Third Report of Sub-Committee "A".

CAPTAIN SAFFORD read the report, and after considerable discussion, the Committee agreed to amend the report as follows:

1. Amend paragraph 4 to read as follows:

"4. With the introduction of the new BCM crypto principle, the following operating facilities will be available:

- (a) Texts consisting either of 26 letters plus space but not including numerals, or, alternatively, of 10 numerals plus one additional symbol plus space but not including letters, may be encrypted. On decryption "7" will print as "X" as with the present CCM.
- (b) None of the additional facilities, for example, a mixture of letters and figures, offered by a standard Teleprinter will be available."

2. Amend paragraph 5 to read as follows:

"5. The U.S. and the British are currently building new off-line cypher machines capable of employing the 7-rotor BCM principle and offering some or all of the facilities inherent in standard Teleprinters. The technique by which these facilities will be provided is different in the U.S. design from that employed in the British design, due to differences in operating requirements, as set forth in paragraphs 7 and 8, below."

3. Amend paragraph 6, in part, as follows:

"6. Both nations are agreed that the following general requirements, if possible, be met:"

4. Amend paragraph 7 as follows:

"7. The British Operational Staff require that off-line machines which are to provide automatic encryption and decryption shall be capable of:

~~TOP SECRET~~

"(a) Accepting a tape, perforated on any Teleprinter employing the International Telegraph Alphabet No. 2. (See page 265, Telegraph Regulations, Cairo Revision of 1938)

"(b) Presenting automatically in page form the decrypted version identical with the original text. Thus, for example, all the Teleprinter functions required for tabulation which appeared in the original text must be reproduced during decryption and be capable of operating a standard Teleprinter."

5. Paragraph 8 - Delete "clearly defined" and substitute "exactly specified".

6. Amend paragraph 8a. and 8b. to read as follows:

"(a) Use some but not all of the upper case characters. (Numbers and slant-mark are used)"

"(b) Insert "Carriage Return" and "Line Feed" during decryption only at the end of each line. Thus the originator's tabulation cannot be reproduced."

7. Amend paragraph 9 to read as follows:

"9. On 20 October a working party of Subcommittee A visited the Teletype Corporation to inspect and discuss the U.S. 'PCM' in the hope that some means might be devised whereby the U.S. cipher machine 'PCM' plus the CSP 5000 (Automatic Off-Line Equipment) and the British cipher machines 'PENDRAGON' or 'SINGLET' could interwork, while still being capable of working with existing cipher machines of the nation concerned and also providing the facilities required by that nation."

8. Delete paragraph 10(a), and reletter subparagraphs 10(b) to read 10(a), 10(c) to read 10(b), 10(d) to read 10(c), 10(e) to read 10(d), and 10(f) to read 10(e).

9. Paragraph 10(a) - Insert "functions, upper case characters, and other" between "Teleprinter" and "facilities".

10. Paragraph 10(c) - Delete "as a matter of urgency".

~~TOP SECRET~~

~~TOP SECRET~~

11. Paragraph 10(d) - Insert "That" before "since" in first line.

12. Amend paragraph 10(e) to read as follows:

"(e) That interchange of views, in particular, on recommendations (b), (c), and (d) above, be continued."

Subject to the foregoing amendments, the Third Report of Sub-Committee "A" was approved by the Executive Committee.

~~TOP SECRET~~

~~TOP SECRET~~**ITEM 4. REPORT ON PATENT PROBLEMS.**

MR. FRIEDMAN stated that Captain Harper had some information pertaining to patent rights to bring before the Committee at this time.

CAPTAIN HARPER remarked that his patent attorney had brought to his attention Article VI and Annex D of the Mutual Defense Assistance Agreement between the United States of America and the United Kingdom of Great Britain and Northern Ireland, which he read as follows:

ARTICLE VI

"1. The two contracting Governments will negotiate appropriate arrangements between them respecting responsibility for claims for the use or infringement of inventions covered by patents or patent applications, trademarks, or copyrights, or other similar claims arising from the use of devices, processes, or technological information in connection with equipment, materials, or services furnished pursuant to this Agreement, or furnished in the interests of production undertaken by agreement between the two contracting Governments in implementation of the pledges of self-help and mutual aid contained in the North Atlantic Treaty.

ANNEX D

"During the course of the negotiations of the Mutual Defense Assistance Agreement, the representatives of the two contracting Governments have reached the understanding that the following points will be considered in the negotiations provided for in Article VI:

(a) The inclusion of an undertaking whereby each contracting Government would assume the responsibility for all the patent or similar claims of its nationals referred to in Article VI of the said Agreement and for such claims arising in its jurisdiction of nationals of any country not a party to this Agreement.

(b) The terms on which inventions would be communicated to contractors with a view to protecting the commercial rights of inventors.

(c) Rights in improvements or other modifications of patented inventions.

~~TOP SECRET~~

"(d) Arrangements for the protection of secret processes and secret technological information, as distinct from patented and patentable inventions.

(e) The system for disclosing the users and the extent of the use of the patents, trade secrets and copyrights referred to in Article VI."

CAPTAIN HARPER added that he had discussed the matter further with the Army's Judge Advocate General's Department, and that they were of the opinion that disclosures of patents, or inventions covered by patent applications, would be to the benefit of the United States Government, and consistent with the rights which the United States Government would normally hold.

MR. FRIEDMAN remarked that he had a memorandum from Captain Harper's patent attorney which was consistent with the information that Captain Harper had just presented. He read the memorandum to the Executive Committee as follows:

"1. The latest formal agreement specifically delineating the rights and duties of the United States and British Governments relative to patents and inventions was the so-called Patent Interchange Agreement, now expired.

2. The Mutual Defense Assistance Treaty of 1950 (Atlantic Pact) contains a clause obligating the United States and the United Kingdom to negotiate a new agreement on such matters - and there is a belief current in the Pentagon that any new undertaking will be very similar to the Patent Interchange Agreement, but no new arrangement has as yet been executed.

3. In the absence of a specific understanding, it is the view of the Army JAG and the Legal Division of the Signal Corps that the conventional license obtained by the Government from its own employees as well as from contractors, which license permits manufacture and use for governmental purposes, justifies the conveyance of technical information as well as equipments involving inventions covered by United States patents or patent applications. The view of the groups mentioned is, in other words, that governmental use is virtually synonymous with governmental advantage.

~~TOP SECRET~~

"4. As far as is known in the Office of the JAG, notwithstanding large and varied shipments of equipment to foreign countries during and following World War II, no cases have arisen in the courts which could result in a judicial determination of the indicated interpretation of the expression governmental use."

CAPTAIN SAFFORD remarked that he would like to bring up a new subject before going on to the next item on the agenda. He made reference to paragraph 7d of the First Report of Sub-Committee "A" dated 26 September 1950 which read as follows:

"d. Rotors on both U.S. and British versions of the 7-rotor BCM to be physically and cryptographically interchangeable. This means that manufacturing, and wiring details to be furnished to the British for this purpose."

CAPTAIN SAFFORD continued by explaining that at the time the report was written, it was proposed that the British would use the TYPEX adapter developed by Commander Seiler, but that since the visit to the Teletype Corporation, Mr. Miller and the other engineers had decided to use the ready-made unit rather than the one developed by Commander Seiler, and that in view of the foregoing, it would be preferable to use 2½" rotors and make them standard throughout the British Service.

MR. MILLER remarked that on the draft report to the U.S. and British Chiefs of Staff, about to come before the Committee for consideration, he was in complete agreement with Captain Safford. He continued by emphasizing that he did not desire to commit the British at this time, but would like to reconsider the matter as a whole. He added that he would be happy to standardize on one or the other, i.e., either the CSP 1700 or the PCM.

MR. FRIEDMAN inquired of Mr. Miller if he would suggest some specific changes in wording of the draft report.

MR. MILLER replied that this item should override the agreement in the earlier one, and that such should be reflected in the minutes.

Before proceeding to the next item on the agenda, MR. FRIEDMAN inquired if there were any comments on the completed First Report of Sub-Committee "B".

~~TOP SECRET~~

~~TOP SECRET~~

DR. SINKOV pointed out that in Appendix "A", AFSAM 7, under the heading "Cryptographic Features" the 1st line should read "Eight 36 point rotors".

MR. FRIEDMAN inquired about the word "permitting".

DR. SINKOV replied that the wording had been suggested by Colonel Henn-Collins, and that the U.S. wording would be "literal cipher machine".

ADMIRAL STONE inquired if there were certain terms in the paper which might make it advisable to prepare a glossary.

DR. SINKOV replied that most of the words could be found in the current confidential list of agreed terms, and therefore, he saw no need for a glossary.

MR. FRIEDMAN pointed out that some of the Appendices had headlines and that some of them did not.

MR. MILLER explained that they had been compiled in great haste, and that it had been agreed that in order to publish them as soon as possible, standardization would not be required.

MR. FRIEDMAN suggested that the paper be turned over to members of Sub-Committee "B" for the purpose of resolving the discrepancies by the time of the final meeting.

MR. MILLER observed that he was the only remaining British member of the Committee.

DR. SINKOV suggested that perhaps Mr. Douglas could represent the U. S. members of the Committee for this purpose.

~~TOP SECRET~~

~~TOP SECRET~~

ITEM 5. CONSIDERATION OF THE PROPOSED REPORT TO THE U.S. AND U.K. JOINT CHIEFS OF STAFF BY THE BRUSA COMMUNICATIONS SECURITY CONFERENCE.

MR. FRIEDMAN thanked Mr. Miller for his assistance in preparing the two draft reports to the British and U.S. Chiefs of Staff, and suggested that the report on the replacement of the CCM be considered at this time.

The Executive Committee agreed that the following amendments would be made to the report:

1. Amend the title to read: "REPORT TO THE BRITISH AND US CHIEFS OF STAFF BY THE BRITISH/US COMMUNICATION SECURITY CONFERENCE ON THE REPLACEMENT OF THE CCM, SEPTEMBER 1950."

2. Amend paragraph 1. to read as follows:

"1. As agreed by the British and US Chiefs of Staff* a British/US Conference to consider the replacement of the existing Combined Cypher Machine opened in Washington on 21 September 1950, as a result of which the Senior British Representative recommends that the British Chiefs of Staff accept the offer by the U.S. Chiefs of Staff of the 7-rotor BCM principle as the long-term solution of the replacement for the present combined cipher machine (CCM)."

3. Amend paragraph 2. to read as follows:

"2. Many related cryptographic devices and features were demonstrated and discussed. Summaries of the proceedings at these meetings have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London. In our estimation this Conference has been of unquestioned value in the field of Combined Communications Security."

4. Amend paragraph 3, in part, as follows:

"3. It is recommended:

- (a) That immediately and on a continuing basis there be complete interchange of technical details of the devices discussed in this Conference. This should include technical visits."

~~TOP SECRET~~

~~TOP SECRET~~

5. Amend paragraph 4 as follows:

"4. The general recommendations in paragraph 3 above together with the detailed technical recommendations of the conference which are attached as Appendix A to this report are submitted for approval by the British and U.S. Chiefs of Staff."

6. Appendix A, amend title to read "TECHNICAL RECOMMENDATIONS".

7. Appendix A, delete "7-rotor BCM" wherever appearing in the Appendix, and substitute "BRUTUS".

8. Appendix A, Replacement of the Existing CCM.

a. Amend paragraph (a) to read as follows:

"(a) That the cryptographic principles of the 7-rotor BCM (cryptosystem BRUTUS) be adopted as a replacement for the CCM in combined communications."

b. Amend paragraph (d) to read as follows:

"(d) That insofar as practicable rotors of U.S. and British versions of the BRUTUS cryptosystem be physically and cryptographically interchangeable and that to this end the British should adopt one or more of the sizes to be used by the U.S. Further, that all data, manufacturing, and wiring details be furnished to the British for this purpose."

9. Appendix A, Temporary Improvement to the Existing CCM.

a. Paragraph (a), delete "henceforth" and substitute "as soon as practicable". Second line, insert "existing" between "each" and "CCM". Delete second sentence. Delete last sentence in parenthesis.

b. Paragraph (b), delete "after suitable rotors become available".

~~TOP SECRET~~

~~TOP SECRET~~

The Executive Committee then agreed that the following amendments would be made to the Report to the British and US Chiefs of Staff by the British/US Communication Security Exploratory Conference:

1. Amend the title to read as follows:

"REPORT TO THE BRITISH AND US CHIEFS OF STAFF BY
THE BRITISH/US COMMUNICATION SECURITY EXPLORATORY
CONFERENCE, SEPTEMBER 1950."

2. Delete "Exploratory Conference for the" from the heading immediately below the title. Subparagraph (e), insert "Communication" between "of" and "Intelligence".

3. Amend paragraph 2 to read as follows:

"2. Summaries of the proceedings at the meetings which followed have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London. In our estimation this conference has been of unquestioned value not only in the field of Combined Communications Security but also in the field of US and British Intra-Communications Security."

4. Amend paragraph 3 to read as follows:

"3. It is recommended:

- (a) That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this conference. This should include technical visits.
- (b) That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF, authentication systems, be authorized.
- (c) That security evaluations be made and exchanged on all items discussed.
- (d) That the U.S.-U.K. JCEC consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.

~~TOP SECRET~~

~~TOP SECRET~~

"(e) That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time."

5. Amend paragraph 4 to read as follows:

"4. The general recommendations in paragraph 3 above together with the detailed conclusions of the Conference which are attached as Appendix A to this report are submitted for the approval of the British and U. S. Chiefs of Staff."

6. Appendix A, paragraph A.(2), Insert "of the foregoing" between "any" and "purpose", changing "purpose" to read "purposes". Before the word "possible" insert "some".

7. Appendix A, paragraph A.(3), amend 2nd sentence to read, in part: "Some possible devices are:"

8. Appendix A, paragraph B, amend to read, in part, as follows:

"B. Merchant Ship Telegraphic Systems

A machine system of at least equivalent security but faster than Cursex, which is under consideration, should replace it, when available, and that such a system should be selected within the next 12 months. Some possible devices are:"

9. Appendix A, paragraph C(2), insert "some" before "possible".

10. Appendix A, paragraph C(3), insert "some" before "possible".

11. Appendix A, paragraph C(3)(b), delete "BCM 7" and substitute "7-rotor BCM".

12. Appendix A, paragraph D(3), insert "Some" before "possible".

~~TOP SECRET~~

~~TOP SECRET~~

13. Appendix A, add new paragraph E as follows:

"E. Teleprinter Systems for the Exchange of Communication Intelligence Material

(1) If there is to be an immediate substitution for ROCKEX a selection can be made from the following machines:

ASAM 2-1

SU.C.O.

(2) Either machine is available in sufficient quantity to meet current requirements in the exchange of intelligence material."

The meeting adjourned at 1717.

~~TOP SECRET~~

~~SECRET~~

BRISA COMSEC CONFERENCE

Executive Committee

AGENDA

For meeting to be held at 1400, 25 October 1950

1. Approval of Final Minutes of Third Executive Committee Meeting.
2. Consideration of Third Report of Subcommittee A.
3. Consideration of Second Report of Subcommittee B.
4. Mr. Friedman's report on patent problems.
5. Consideration of the proposed Report to the U.S. and U.K. Joint Chiefs of Staff by the BRISA Communication Conference.

~~SECRET~~

~~SECRET~~*Mr. Friedman*
AFSA - 00T

18 October 1950

MEMORANDUM FOR MEMBERS OF THE EXECUTIVE COMMITTEE

**SUBJECT: Scheduled Meetings of the Executive Committee, BRUSA
Communication Security Conference**

1. The following meetings of the Executive Committee, BRUSA Communication Security Conference have been scheduled:

1400 25 October 1950. Meeting of Combined Executive Committee

1400 27 October 1950. Final Meeting of Combined Executive Committee

2. Meetings will be held in Room 1212, NAVSECSTA.

3. For your information the final plenary session has been scheduled for 1500, Friday, 27 October 1950, in Room 1212, NAVSECSTA.

William F. Friedman
WILLIAM F. FRIEDMAN,
Chairman, Executive Committee

~~SECRET~~

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCE

MINUTES OF

1

THE THIRD MEETING OF THE EXECUTIVE COMMITTEE

The Third Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1400 on 11 October 1950 in Room 1212, U. S. Navy Security Station, Washington, D. C.

Representatives Present

United States

Mr. W. F. Friedman, Chairman
Rear Admiral Earl E. Stone, USN
Captain L. F. Safford, USN
Captain J. S. Harper, USN
Lt. Col. G. V. Johnson, USA
Lt. Col. R. H. Horton, USA
Major G. E. Parr, USAF
Dr. A. Sinkov

United Kingdom

Mr. T. R. W. Burton Miller
Captain, the Earl Cairns, R.N.
Brigadier John H. Tiltman

Secretariat

Lieutenant J. W. Pearson, USN
Miss Catherine M. Johnson

ITEM 1. APPROVAL OF MINUTES OF FIRST AND SECOND MEETINGS:

MR. FRIEDMAN inquired if there were any comments or corrections to be made to the Minutes of the First and Second Meetings.

There were none.

The Committee approved the minutes of the First and Second Meetings.

MR. FRIEDMAN made reference to a part of the minutes of the First Executive Meeting which read as follows:

"..... making reference to the background statements that he had read at the First Meeting of the Plenary Committee, Mr. Friedman inquired if the British Delegation had any objections or comments to make, particularly with regard to the articles quoted from the agreements."

"Mr. Miller replied that his Delegation had no comments on the articles quoted from the agreements, but that they would like to make certain that they understood them."

He inquired of Mr. Miller as to whether he had had an opportunity to study the articles in question.

MR. MILLER replied in the affirmative, and stated that he would like to make certain that his interpretation of the articles was the same as the U.S. interpretation. He continued by explaining that it was his understanding, that if British Authorities desired to copy something from a U.S. plan or device, they could do so without waiting for detailed negotiations between the two Governments, provided that arrangements were made with regard to patent rights.

MR. FRIEDMAN stated that he thought Mr. Miller was correct, but added that he would like to review Article VI as follows:

"1. The two contracting Governments will negotiate appropriate arrangements between them respecting responsibility for claims for the use or infringement of inventions covered by patents or patent applications, trademarks, or copyrights, or other similar claims

"arising from the use of devices, processes, or technological information in connection with equipment, materials or services furnished pursuant to this Agreement, or furnished in the interests of production undertaken by agreement between the two contracting Governments on implementation of the pledges of self-help and mutual aid contained in the North Atlantic Treaty."

AFSA/
He continued by saying that he had requested the patent section of the Office of Research and Development to make a study which would help to clarify any questions which might arise. He stated that he had not yet received the report, but would have it ready for presentation at the next meeting of the Executive Committee.

CAPTAIN HARPER remarked that he thought that it was generally considered that experimentation was the same as research, and as such did not come within the scope of patent rights. He added that patent rights pertained to construction or use for commercial purposes.

MR. MILLER agreed, but stated that he was of the opinion that the matter went further than that; he explained that he thought that one Government might copy the patents of the other, as long as the patent copied were used for purely governmental service. He continued by saying that patent rights were involved when a Government sells the patent to a commercial firm, or when they try to profit from it.

MR. FRIEDMAN commented that the understanding that U.S. Authorities had with respect to the protection of information was that it would not be published in a journal. He stated that he thought the arrangement was of a reciprocal nature, that is, if the British Government desired to incorporate certain things for purely British Governmental use from ideas covered by U.S. patents, then the U.S. Government would be free to make similar use of ideas covered by British patents.

CAPTAIN HARPER stated that he wasn't sure if Mr. Friedman's remarks were entirely correct. He pointed out that some patents were taken out in an individual's name, and the Government was given full and free use of them, but that this didn't mean that the opposite government would have free usage of them. He added that probably the same thing was true from a British standpoint.

CAPTAIN SAFFORD remarked that the Government had the right to transfer the use of a patent to another Government on its own terms.

MR. FRIEDMAN stated that there was a paragraph in the Lend-Lease Law to the effect that the U.S. Government would undertake to protect the rights of inventors under the Lend-Lease arrangements. He added that he thought it a question for the legal people to answer.

CAPTAIN HARPER stated, for the sake of the record, that he was of the opinion that the usage of any idea for research purposes is unrestricted except as to publication for the sake of security.

MR. FRIEDMAN stated that he thought that, in any event, many precedents could be found from World War II. He reiterated that he would have the report from the legal section which he would present to the Committee at the next Meeting.

~~TOP SECRET~~ITEM 2. CONSIDERATION OF THE SECOND REPORT OF SUBCOMMITTEE "A".

MR. FRIEDMAN requested Captain Safford to present the second report of Sub-Committee "A".

CAPTAIN SAFFORD recalled that the first report of Sub-Committee "A" had covered the encryption of literal texts. He remarked that the next item that the Committee had considered was the question of the encryption of numerals plus "X" or "Slash" for purposes of weather, and pointed out that the Committee had agreed that the necessary facility should be provided as soon as it is available, where required.

With respect to Encryption of Letters, Plus Numerals, Plus Certain Other Teleprinter Characters, Captain SAFFORD stated that the Committee had not been able to come to complete agreement due to the fact that different operational requirements were involved. He continued by saying that a possible compromise between these conflicting developments had recently been put forward from the U. S. side, and a working party consisting of himself, Commander Seiler, Commander Linn, Lt. Col. Henn-Collins, and Mr. Jolley had been appointed to investigate the proposal. He added that on Friday, 20 October 1950, he planned to escort the British members of the working party on a visit to the Teletype Corporation where the PCM (CSP 4700) and the new Off-Line Automatic Equipment (CSP 5000) were under development, and that the working party would resume its discussions on Monday, 23 October 1950, and would report in due course to Sub-Committee "A". He pointed out that this was the only point to be cleared up, and that it would necessitate the reconvening of Sub-Committee "A" for the purpose of rendering a final report and recommendations on this point alone; he remarked that if no firm understanding could be reached, then Sub-Committee "A" would have to submit some kind of a recommendation to defer decision for approximately a year.

In the way of explanation, MR. MILLER pointed out that British operational people had asked for encipherment of the whole teletypewriter series, but that the U. S. requirement was basically for the encipherment of letters and numerals only.

MR. FRIEDMAN inquired of Captain Safford if this would apply to the BCM.

CAPTAIN SAFFORD replied that it would have application to the new BCM. He explained that agreement had been reached on the BCM principle, and that it had been accepted as far as the CSP 4800 was concerned. He pointed out that the BCM had been accepted, and that it would be sent to London with no strings attached, but that this other matter was in addition to that in

~~TOP SECRET~~

~~TOP SECRET~~

that it was being recommended that they go one step further, and make provisions for the encipherment of numerals, "X" or "Slash".

CAPTAIN SAFFORD commented that the next report of Sub-Committee "A" would deal with the matter in greater detail. He pointed out that the Army and Navy desired a smaller and lighter machine, and that, particularly from a Navy standpoint, it would be advantageous to use the same machine for low as well as high echelon applications.

ADMIRAL STONE remarked, that since this matter remained to be cleared up, he saw no reason for having the Executive and Plenary Meetings scheduled for Friday.

CAPTAIN SAFFORD commented that while the remaining point was a small one in itself, it was a very important one with respect to the construction of the machine.

DR. SINKOV stated that since the working group would deal altogether with the exchange of information on the COMINT side, it might be well to close the work of Sub-Committee "B" by transferring the teleprinter problem to the next Conference.

MR. FRIEDMAN replied that he did not believe such action would be valid, since the COMSEC Conference had been authorized by the Joint Chiefs of Staff only for the exchange of cryptographic principles, and for action in regard to a replacement for the CCM. This view was shared by other members of the Executive Committee.

MR. FRIEDMAN then stated that if it were agreeable to the Committee the Executive and Plenary Committee Meetings scheduled for 13 October 1950 would be cancelled.

The Committee agreed.

MR. MILLER stated that it was his understanding that after Sub-Committee "A" had submitted its 3rd report, and after Sub-Committee "B" had submitted its 2nd report, then there would be a final meeting of the Executive and Plenary Committees.

MR. FRIEDMAN agreed, and inquired if the Committee approved the Second Report of Sub-Committee "A".

~~TOP SECRET~~

CAPTAIN HARPER suggested that the use of PCM in the report might be confusing to both British and U. S. representatives. He pointed out that PCM meant "pulse code modulation", which was used in a considerable number of machines.

MR. MILLER remarked that if quotation marks were placed around PCM it would be acceptable to him.

MR. FRIEDMAN suggested that the abbreviation MBCM be used in place of PCM; he requested Captain Safford to comment.

CAPTAIN SAFFORD explained that the machine had been called a miniature cipher machine, and that the word "portable" had been used to describe the machine due to the lack of a better word. He added that they had not been concerned with the "pulse code modulation".

DR. SINKOV suggested that the parens be removed from around "CSP 4700", and that PCM be deleted altogether.

ADMIRAL STONE remarked that he had seen the title BCM - 7 used in one of the papers, and suggested that possibly BCM-7S would be an appropriate designation.

CAPTAIN HARPER observed that SBCM might be a better designation.

CAPTAIN SAFFORD stated that the designation used in contracts with the Teletype Corporation was PCM.

DR. SINKOV pointed out that PCM was used in the report of Sub-Committee "B" as well as in the report under consideration, and that he thought it might be well to be consistent throughout.

MR. FRIEDMAN inquired if the Committee were agreeable to adopting Mr. Miller's suggestion, viz, that quotation marks be placed around the designation PCM throughout both reports.

The Committee agreed.

MR. FRIEDMAN then asked if the Committee were agreeable to accepting the Second Report of Sub-Committee "A", as amended.

The Committee agreed to accept the report as amended.

MR. MILLER recalled that a suggestion had been made that a common title for the 7-rotor BCM crypto-technique be adopted, and that the codeword "BRUTUS" had been proposed. He explained that he had signalled GCHQ in the premises, and had received a favorable reply. He added that he felt that this matter came under the cognizance of Sub-Committee "A" but stated that it might be well for the Executive Committee to know that the word was acceptable to the British.

~~TOP SECRET~~

CAPTAIN SAFFORD stated that he could not state definitely, but that it was his understanding that "BRUTUS" was being used elsewhere in the U. S. Armed Forces, however, he added that it was not used crypto-wise.

ADMIRAL STONE suggested that the U. S. delegation accept the word "BRUTUS" subject to determining whether it is already being used.

CAPTAIN SAFFORD recommended that the word "AJAX" be adopted as the designation for the present CCM in any of its forms. He inquired whether Mr. Miller could request clearance on "AJAX" as well.

MR. MILLER replied in the affirmative, stating that he would do so by signal.

MR. FRIEDMAN inquired if the Committee were agreeable to proceeding on the basis that "BRUTUS" would be adopted as the designation for the 7-rotor BCM crypto-technique, subject to the determination that no conflict exists in U. S. terminology; and that "AJAX" would be adopted as the designation for the present CCM in any of its forms, subject to the determination that no conflict exists in British terminology.

The Committee so agreed.

CAPTAIN, THE EARL CAIRNS inquired if the aforementioned designations would be stamped on the machines.

CAPTAIN SAFFORD replied that they would be used in an unrestricted status in correspondence, on key lists, instructions, and name plates.

MR. MILLER inquired if the word "AJAX" would signify the 5-rotor CCM crypto-technique employing standard rotors with non-rotating cam-contours.

DR. SINKOV replied in the negative, explaining that "AJAX" denoted the basic crypto system regardless of the rotors involved.

MR. FRIEDMAN remarked that certain "AJAX" crypto techniques might be interchangeable with another "AJAX" using the same cam contours. He pointed out that if one didn't use them and the other did, it might result in confusion.

MR. MILLER commented that it had been agreed that rotors should be standardized insofar as the BCM was concerned. He explained that the PCM machine included the BCM technique but that the British would not want the responsibility for producing rotors of the size presently employed in the PCM.

~~TOP SECRET~~

~~TOP SECRET~~

DR. SINKOV stated that he thought that Mr. Miller was speaking of two wholly different concepts of the word "BRUTUS" as applied to a crypto system which uses a different mechanism. He added that it might call for different size rotors.

MR. MILLER replied that "BRUTUS" was employed in both the PCM and BCM, and inquired if it were agreed that only BCM rotors would be interchangeable between the British and U. S.

MR. FRIEDMAN inquired of Mr. Miller if he desired a note in the record to the effect that he (Mr. Miller) was not prepared to commit himself regarding the interchangeability of BCM and PCM rotors.

MR. MILLER replied in the affirmative.

CAPTAIN SAFFORD remarked that as far as the PCM was concerned, there was no reason for believing that the rotors would be any different from anything else.

~~TOP SECRET~~

ITEM 3. CONSIDERATION OF THE FIRST REPORT OF SUBCOMMITTEE "B".

MR. FRIEDMAN requested Dr. Sinkov to present the first report of Sub-Committee "B".

DR. SINKOV stated that he regretted that the report had not been available at an earlier date, but explained that the last meeting of the Sub-Committee had been held the previous day. He pointed out that the report was not yet complete in that brief descriptions of the equipments mentioned were being prepared, and would be attached to the report as appendices. He then read the report to the Committee.

Making reference to paragraph 2 of the report, Captain SAFFORD inquired if there were any reason for omitting the Stromberg-Carlson TSS Ciphony System from that list. He pointed out that there was no technical description of the equipment available at this time.

MR. MILLER inquired if there would be an opportunity to discuss this equipment or to demonstrate it.

CAPTAIN SAFFORD replied that it would be very worthwhile to have Lt. Col. Henn-Collins examine the equipment.

DR. SINKOV pointed out that a number of equipments had been discussed without having been seen, and suggested that someone who is familiar with the device might explain its design principles and operation.

MR. MILLER suggested that this item be included in the second report of Sub-Committee "B".

ADMIRAL STONE said that he thought Dr. Sinkov and Captain Safford should examine the facts, and bring the matter up at the next meeting.

MR. FRIEDMAN inquired if the Committee were agreeable to including this item in the next report of Sub-Committee "B".

The Committee so agreed.

The Executive Committee considered the first report of Sub-Committee "B" in its entirety. As a result of this consideration it was agreed that the following changes would be made (Comments are included where appropriate):

1. Title - Change to read: "First Report of Sub-Committee "B" to the Executive Committee."

2. Paragraph 1a - amend to read:

a. "Low Echelon (including minor war vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services."

3. Paragraph 2 - amend to read as follows:

"2. During the course of the discussion and demonstrations 33 crypto systems were considered. Technical descriptions of 29 of these are included in the appendices as follows:

	<u>MACHINES</u>	<u>CIFAX</u>	<u>CIPHONY</u>	<u>HAND SYSTEMS</u>
U.S.	a. AFSAM 7 b. AFSAM 9 c. 7 Rotor BCM d. "PCM" e. MCM	f. ASAX 2 g. NRL Cifax	h. ASAY 4 i. ASAY 6 j. ASAY 8 k. AN/TRA 16 l. TSS	m. ASAD 1 n. Running Key Cipher
U.K.	o. Mercury p. Concert q. Rollick r. Singlet s. Pendragon t. DUP 1	u. METFAX	v. Hallmark w. Sorcerer x. D 70	y. Playfex z. Linex aa. Cursex bb. Otmetco cc. Alametco

"Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries. Brief mention was made of a modification of the M-209 which has been proposed by Hagelin. A description which he has submitted is included in the appendix. The appendix also includes some miscellaneous notes on general items."

4. Paragraph 3 - amend to read as follows:

"3. None of these cryptosystems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations during the interim between the close of this conference and the opening of the next."

5. Paragraph 4 - add the following sentence at the end of the paragraph:

"This agreement would limit the number of different types of rotors employed and thereby facilitate the interchangeability between U.K. and U.S. sources."

6. Paragraph 5A - amend to read in part as follows:

"A. Low Echelon (including Minor War Vessels) Telegraphic systems - including combined assault codes and tactical systems for all military Services."

7. Paragraph 5A3 - amend to read as follows:

"3. We note that both US and UK have a number of new machine systems under development, but that none of these is likely to be available for general combined use before 1954."

8. Paragraph 5A4a - amend to read as follows:

"a. No machine system is likely to be available for general combined use before 1954."

9. Paragraph 5A4b - delete "devices" and substitute "systems".

10. Paragraph 5A4c - enclose PCM in quotation marks.

11. Paragraph 5B2 - amend to read as follows:

"2. We recommend that a machine system of at least equivalent security but faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

"PCM"
DUP 1
AFSAM 7
MCM"

12. Paragraph 5C3 - amend to read as follows:

"3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for general combined use before 1954."

~~TOP SECRET~~

13. Paragraph 5C5a - delete ", say, 1953." and substitute "1954."
14. Paragraph 5C5b(2) - add "Pencil and paper system for very low echelon purposes."
15. Paragraph 5C5b(3) - delete "(to be described under Item E)".
16. Paragraph 5C5c(2) - enclose PCM in quotation marks. Add following to end of list: "Pencil and paper systems."
17. Paragraph 5C5c(4) - amend to read as follows:
- "(4) Cifax - ASAX 2
NRL Cifax
METFAX"
18. Paragraph 5C5c - delete "this category" from the Note at the end, and substitute "category (4)".
19. Paragraph 5D2 - amend to read as follows:
- "2. We note that both the UK and the US have a number of new systems under development but that none of these is likely to be available for general combined use before 1954."
20. Paragraph 5D3a - delete ", say, 1953." and substitute "1954."
21. Paragraph 5D3c(1) - insert "can be used only" between "attachment;" and "over".
22. Paragraph 5D3c(3) - delete "tactical" and substitute "tactical".
23. Paragraph 6 - amend to read as follows:
- "6. The Sub-Committee has the following recommendations to make:
- "a. That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this exploratory conference. This should include technical visits.

~~TOP SECRET~~

"b. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.

"c. That security evaluations be made and exchanged on all items discussed.

"d. That a copy of the final report of the conference be submitted to the U.S.-U.K. JCEC and that the U.S.-U.K. JCEC be requested to consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.

"e. That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time."

With respect to future meetings, MR. MILLER suggested that the Executive Committee meet after Sub-Committee "B" had made its second report so that if the working group had anything of interest to report, they could do so at that time. He added that it might be desirable to pass a copy of the conclusions to the COMINT Conference for their information. He pointed out that he saw no need for the Executive Committee to meet again until after the Sub-Committees had submitted their next reports, which would be sometime after 23 October 1950.

MR. FRIEDMAN inquired if there were any objections to Mr. Miller's suggestions.

There were none.

The meeting adjourned at 1625.

~~TOP SECRET~~

1

MEMORANDUM FOR THE MEMBERS OF THE EXECUTIVE COMMITTEE:

Subject: Tentative Minutes of the Third Meeting.

1. The subject minutes are forwarded herewith for your consideration.

2. Please advise the Secretariat, located in Room 19-211, U. S. Navy Security Station, (Telephone: Code 131, extension 60354) of your comments and/or concurrence.



J. W. PEARSON
H. D. JONES
Secretariat

~~TOP SECRET~~

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCE

MINUTES OF

THE THIRD MEETING OF THE EXECUTIVE COMMITTEE

The Third Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1400 on 11 October 1950 in Room 1212, U. S. Navy Security Station, Washington, D. C.

Representatives Present

United States

United Kingdom

Mr. W. F. Friedman, Chairman
Rear Admiral Earl E. Stone, USN
Captain L. F. Safford, USN
Captain J. S. Harper, USN
Lt. Col. G. V. Johnson, USA
Lt. Col. R. H. Horton, USA
Major G. E. Parr, USAF
Dr. A. Sinkov

Mr. T. R. W. Burton Miller
Captain, the Earl Cairns, R.N.
Brigadier John H. Tiltman

Secretariat

Lieutenant J. W. Pearson, USN
Miss Catherine W. Johnson

ITEM 1. APPROVAL OF MINUTES OF FIRST AND SECOND MEETINGS:

MR. FRIEDMAN inquired if there were any comments or corrections to be made to the Minutes of the First and Second Meetings.

There were none.

The Committee approved the minutes of the First and Second Meetings.

MR. FRIEDMAN made reference to a part of the minutes of the First Executive Meeting which read as follows:

"..... making reference to the background statements that he had read at the First Meeting of the Plenary Committee, Mr. Friedman inquired if the British Delegation had any objections or comments to make, particularly with regard to the articles quoted from the agreements."

"Mr. Miller replied that his Delegation had no comments on the articles quoted from the agreements, but that they would like to make certain that they understood them."

He inquired of Mr. Miller as to whether he had had an opportunity to study the articles in question.

MR. MILLER replied in the affirmative, and stated that he would like to make certain that his interpretation of the articles was the same as the U.S. interpretation. He continued by explaining that it was his understanding, that if British Authorities desired to copy something from a U.S. plan or device, they could do so without waiting for detailed negotiations between the two Governments, provided that arrangements were made with regard to patent rights.

MR. FRIEDMAN stated that he thought Mr. Miller was correct, but added that he would like to review Article VI as follows:

"1. The two contracting Governments will negotiate appropriate arrangements between them respecting responsibility for claims for the use or infringement of inventions covered by patents or patent applications, trademarks, or copyrights, or other similar claims

"arising from the use of devices, processes, or technological information in connection with equipment, materials or services furnished pursuant to this Agreement, or furnished in the interests of production undertaken by agreement between the two contracting Governments on implementation of the pledges of self-help and mutual aid contained in the North Atlantic Treaty."

He continued by saying that he had requested the patent section of the Office of Research and Development to make a study which would help to clarify any questions which might arise. He stated that he had not yet received the report, but would have it ready for presentation at the next meeting of the Executive Committee.

CAPTAIN HARPER remarked that he thought that it was generally considered that experimentation was the same as research, and as such did not come within the scope of patent rights. He added that patent rights pertained to construction or use for commercial purposes.

MR. MILLER agreed, but stated that he was of the opinion that the matter went further than that; he explained that he thought that one Government might copy the patents of the other, as long as the patent copied were used for purely governmental service. He continued by saying that patent rights were involved when a Government sells the patent to a commercial firm, or when they try to profit from it.

MR. FRIEDMAN commented that the understanding that U.S. Authorities had with respect to the protection of information was that it would not be published in a journal. He stated that he thought the arrangement was of a reciprocal nature, that is, if the British Government desired to incorporate certain things for purely British Governmental use from ideas covered by U.S. patents, then the U.S. Government would be free to make similar use of ideas covered by British patents.

CAPTAIN HARPER stated that he wasn't sure if Mr. Friedman's remarks were entirely correct. He pointed out that some patents were taken out in an individual's name, and the Government was given full and free use of them, but that this didn't mean that the opposite government would have free usage of them. He added that probably the same thing was true from a British standpoint.

CAPTAIN SAFFORD remarked that the Government had the right to transfer the use of a patent to another Government on its own terms.

MR. FRIEDMAN stated that there was a paragraph in the Lend-Lease Law to the effect that the U.S. Government would undertake to protect the rights of inventors under the Lend-Lease arrangements. He added that he thought it a question for the legal people to answer.

CAPTAIN HARPER stated, for the sake of the record, that he was of the opinion that the usage of any idea for research purposes is unrestricted except as to publication for the sake of security.

MR. FRIEDMAN stated that he thought that, in any event, many precedents could be found from World War II. He reiterated that he would have the report from the legal section which he would present to the Committee at the next Meeting.

~~TOP SECRET~~ITEM 2. CONSIDERATION OF THE SECOND REPORT OF SUBCOMMITTEE "A".

MR. FRIEDMAN requested Captain Safford to present the second report of Sub-Committee "A".

CAPTAIN SAFFORD recalled that the first report of Sub-Committee "A" had covered the encryption of literal texts. He remarked that the next item that the Committee had considered was the question of the encryption of numerals plus "X" or "Slash" for purposes of weather, and pointed out that the Committee had agreed that the necessary facility should be provided as soon as it is available, where required.

With respect to Encryption of Letters, Plus Numerals, Plus Certain Other Teleprinter Characters, Captain SAFFORD stated that the Committee had not been able to come to complete agreement due to the fact that different operational requirements were involved. He continued by saying that a possible compromise between these conflicting developments had recently been put forward from the U. S. side, and a working party consisting of himself, Commander Seiler, Commander Linn, Lt. Col. Henn-Collins, and Mr. Jolley had been appointed to investigate the proposal. He added that on Friday, 20 October 1950, he planned to escort the British members of the working party on a visit to the Teletype Corporation where the PCM (CSP 4700) and the new Off-Line Automatic Equipment (CSP 5000) were under development, and that the working party would resume its discussions on Monday, 23 October 1950, and would report in due course to Sub-Committee "A". He pointed out that this was the only point to be cleared up, and that it would necessitate the reconvening of Sub-Committee "A" for the purpose of rendering a final report and recommendations on this point alone; he remarked that if no firm understanding could be reached, then Sub-Committee "A" would have to submit some kind of a recommendation to defer decision for approximately a year.

In the way of explanation, MR. MILLER pointed out that British operational people had asked for encipherment of the whole teletypewriter series, but that the U. S. representatives desired the encipherment of numerals only.

MR. FRIEDMAN inquired of Captain Safford if this would apply to the BCM.

CAPTAIN SAFFORD replied that it would have application to the new BCM. He explained that agreement had been reached on the BCM principle, and that it had been accepted as far as the CSP 4800 was concerned. He pointed out that the BCM had been accepted, and that it would be sent to London with no strings attached, but that this other matter was in addition to that in

~~TOP SECRET~~

that it was being recommended that they go one step further, and make provisions for the encipherment of numerals, "X" or "Slash".

MR. MILLER pointed out that British operational people had asked for a machine which would provide encipherment of upper and lower cases, both letters and numerals, but that the U.S. operational people did not desire full teleprinter accommodations in that they were only interested in the lower case.

CAPTAIN SAFFORD commented that the next report of Sub-Committee "A" would deal with the matter in greater detail. He pointed out that the Army and Navy desired a smaller and lighter machine, and that, particularly from a Navy standpoint, it would be advantageous to use the same machine for low as well as high echelon applications.

ADMIRAL STONE remarked, that since this matter remained to be cleared up, he saw no reason for having the Executive and Plenary Meetings scheduled for Friday.

CAPTAIN SAFFORD commented that while the remaining point was a small one in itself, it was a very important one with respect to the construction of the machine.

DR. SINKOV stated that since the working group would deal altogether with the exchange of information on the COMINT side, it might be well to close the work of Sub-Committee "B" by transferring the teleprinter problem to the next Conference.

MR. FRIEDMAN replied that he did not believe such action would be valid, since the COMSEC Conference had been authorized by the Joint Chiefs of Staff only for the exchange of cryptographic principles, and not for action in regard to a replacement for the CCM. This view was shared by other members of the Executive Committee.

MR. FRIEDMAN then stated that if it were agreeable to the Committee the Executive and Plenary Committee Meetings scheduled for 13 October 1950 would be cancelled.

The Committee agreed.

MR. MILLER stated that it was his understanding that after Sub-Committee "A" had submitted its 3rd report, and after Sub-Committee "B" had submitted its 2nd report, then there would be a final meeting of the Executive and Plenary Committees.

MR. FRIEDMAN agreed, and inquired if the Committee approved the Second Report of Sub-Committee "A".

CAPTAIN HARPER suggested that the use of PCM in the report might be confusing to both British and U. S. representatives. He pointed out that PCM meant "pulse code modulation", which was used in a considerable number of machines.

MR. MILLER remarked that if quotation marks were placed around PCM it would be acceptable to him.

MR. FRIEDMAN suggested that the abbreviation MBCM be used in place of PCM; he requested Captain Safford to comment.

CAPTAIN SAFFORD explained that the machine had been called a miniature cipher machine, and that the word "portable" had been used to describe the machine due to the lack of a better word. He added that they had not been concerned with the "pulse code modulation".

DR. SINKOV suggested that the parens be removed from around "CSP 4700", and that PCM be deleted altogether.

ADMIRAL STONE remarked that he had seen the title BCM - 7 used in one of the papers, and suggested that possibly BCM-7S would be an appropriate designation.

CAPTAIN HARPER observed that SBCM might be a better designation.

CAPTAIN SAFFORD stated that the designation used in contracts with the Teletype Corporation was PCM.

DR. SINKOV pointed out that PCM was used in the report of Sub-Committee "B" as well as in the report under consideration, and that he thought it might be well to be consistent throughout.

MR. FRIEDMAN inquired if the Committee were agreeable to adopting Mr. Miller's suggestion, viz, that quotation marks be placed around the designation PCM throughout both reports.

The Committee agreed.

MR. FRIEDMAN then asked if the Committee were agreeable to accepting the Second Report of Sub-Committee "A", as amended.

The Committee agreed to accept the report as amended.

MR. MILLER recalled that a suggestion had been made that a common title for the 7-rotor BCM crypto-technique be adopted, and that the codeword "BRUTUS" had been proposed. He explained that he had signalled GCHQ in the premises, and had received a favorable reply. He added that he felt that this matter came under the cognizance of Sub-Committee "A" but stated that it might be well for the Executive Committee to know that the word was acceptable to the British.

CAPTAIN SAFFORD stated that he could not state definitely, but that it was his understanding that "BRUTUS" was being used elsewhere in the U. S. Armed Forces, however, he added that it was not used crypto-wise.

ADMIRAL STONE suggested that the U. S. delegation accept the word "BRUTUS" subject to determining whether it is already being used.

CAPTAIN SAFFORD recommended that the word "AJAX" be adopted as the designation for the present CCM in any of its forms. He inquired whether Mr. Miller could request clearance on "AJAX" as well.

MR. MILLER replied in the affirmative, stating that he would do so by signal.

MR. FRIEDMAN inquired if the Committee were agreeable to proceeding on the basis that "BRUTUS" would be adopted as the designation for the 7-rotor BCM crypto-technique, subject to the determination that no conflict exists in U. S. terminology; and that "AJAX" would be adopted as the designation for the present CCM in any of its forms, subject to the determination that no conflict exists in British terminology.

The Committee so agreed.

CAPTAIN, THE EARL CAIRNS inquired if the aforementioned designations would be stamped on the machines.

CAPTAIN SAFFORD replied that they would be used in an unrestricted status in correspondence, on key lists, instructions, and name plates.

MR. MILLER inquired if the word "AJAX" would signify the 3-rotor CCM crypto-technique employing standard rotors with non-rotating cam-contours.

DR. SINKOV replied in the negative, explaining that "AJAX" denoted the basic crypto system regardless of the rotors involved.

MR. FRIEDMAN remarked that certain "AJAX" crypto techniques might be interchangeable with another "AJAX" using the same cam contours. He pointed out that if one didn't use them and the other did, it might result in confusion.

MR. MILLER commented that it had been agreed that rotors should be standardized insofar as the BCM was concerned. He explained that if they accept the PCM machine and adapt it to work with the SINGLET, then they would not want the responsibility for standardizing rotors.

DR. SINKOV stated that he thought that Mr. Miller was speaking of two wholly different concepts of the word "BRUTUS" as applied to a crypto system which uses a different mechanism. He added that it might call for different size rotors.

MR. MILLER replied that "BRUTUS" was employed in both the PCM and BCM, and inquired if it were agreed that rotors would be interchangeable for the BCM.

MR. FRIEDMAN inquired of Mr. Miller if he desired a note in the record to the effect that he (Mr. Miller) had no commitment to make with regard to the interchangeability of BCM and PCM rotors.

MR. MILLER replied in the affirmative.

CAPTAIN SAFFORD remarked that as far as the PCM was concerned, there was no reason for believing that the rotors would be any different from anything else.

ITEM 3. CONSIDERATION OF THE FIRST REPORT OF SUBCOMMITTEE "B".

MR. FRIEDMAN requested Dr. Sinkov to present the first report of Sub-Committee "B".

DR. SINKOV stated that he regretted that the report had not been available at an earlier date, but explained that the last meeting of the Sub-Committee had been held the previous day. He pointed out that the report was not yet complete in that brief descriptions of the equipments mentioned were being prepared, and would be attached to the report as appendices. He then read the report to the Committee.

Making reference to paragraph 2 of the report, Captain SAFFORD inquired if there were any reason for omitting the Stromberg-Carlson TSS Ciphony System from that list. He pointed out that there was no technical description of the equipment available at this time.

MR. MILLER inquired if there would be an opportunity to discuss this equipment or to demonstrate it.

CAPTAIN SAFFORD replied that it would be very worthwhile to have Lt. Col. Henn-Collins examine the equipment.

DR. SINKOV pointed out that a number of equipments had been discussed without having been seen, and suggested that someone who is familiar with the device might explain its design principles and operation.

MR. MILLER suggested that this item be included in the second report of Sub-Committee "B".

ADMIRAL STONE said that he thought Dr. Sinkov and Captain Safford should examine the facts, and bring the matter up at the next meeting.

MR. FRIEDMAN inquired if the Committee were agreeable to including this item in the next report of Sub-Committee "B".

The Committee so agreed.

The Executive Committee considered the first report of Sub-Committee "B" in its entirety. As a result of this consideration it was agreed that the following changes would be made (Comments are included where appropriate):

1. Title - Change to read: "First Report of Sub-Committee "B" to the Executive Committee."

2. Paragraph 1a - amend to read:

a. "Low Echelon (including minor war vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services."

3. Paragraph 2 - amend to read as follows:

"2. During the course of the discussion and demonstrations 33 crypto systems were considered. Technical descriptions of 29 of these are included in the appendices as follows:

	<u>MACHINES</u>	<u>CIFAX</u>	<u>CIPHONY</u>	<u>HAND SYSTEMS</u>
	a. AFSAM 7	f. ASAX 2	h. ASAY 4	m. ASAD 1
	b. AFSAM 9	g. NRL Cifax	i. ASAY 6	n. Running Key
U.S.	c. 7 Rotor BCM		j. ASAY 8	Cipher
	d. "PCM"		k. AN/TRA 16	
	e. MCM		l. TSS	
<hr/>				
	o. Mercury	u. METFAX	v. Hallmark	y. Playfex
	p. Concert		w. Sorcerer	z. Linex
U.K.	q. Rollick		x. D 70	aa. Cursex
	r. Singlet			bb. Otmotco
	s. Pendragon			cc. Alametco
	t. DUP 1			

"Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries. Brief mention was made of a modification of the M-209 which has been proposed by Hagelin. A description which he has submitted is included in the appendix. The appendix also includes some miscellaneous notes on general items."

4. Paragraph 3 - amend to read as follows:

"3. None of these cryptosystems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations during the interim between the close of this conference and the opening of the next."

5. Paragraph 4 - add the following sentence at the end of the paragraph:

"This agreement would limit the number of different types of rotors employed and thereby facilitate the interchangeability between U.K. and U.S. sources."

6. Paragraph 5A - amend to read in part as follows:

"A. Low Echelon (including Minor War Vessels) Telegraphic systems - including combined assault codes and tactical systems for all military Services."

7. Paragraph 5A3 - amend to read as follows:

"3. We note that both US and UK have a number of new machine systems under development, but that none of these is likely to be available for general combined use before 1954."

8. Paragraph 5A4a - amend to read as follows:

"a. No machine system is likely to be available for general combined use before 1954."

9. Paragraph 5A4b - delete "devices" and substitute "systems".

10. Paragraph 5A4c - enclose PCM in quotation marks.

11. Paragraph 5B2 - amend to read as follows:

"2. We recommend that a machine system of at least equivalent security but faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

"PCM"
DUP 1
AFSAM 7
MCM"

12. Paragraph 5C3 - amend to read as follows:

"3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for general combined use before 1954."

~~TOP SECRET~~

13. Paragraph 5C5a - delete ", say, 1953." and substitute "1954."
14. Paragraph 5C5b(2) - add "Pencil and paper system for very low echelon purposes."
15. Paragraph 5C5b(3) - delete "(to be described under Item E)".
16. Paragraph 5C5c(2) - enclose PCM in quotation marks. Add following to end of list: "Pencil and paper systems."
17. Paragraph 5C5c(4) - amend to read as follows:
- "(4) Cifax - ASAX 2
NRL Cifax
METFAX"
18. Paragraph 5C5c - delete "this category" from the Note at the end, and substitute "category (4)".
19. Paragraph 5D2 - amend to read as follows:
- "2. We note that both the UK and the US have a number of new systems under development but that none of these is likely to be available for general combined use before 1954."
20. Paragraph 5D3a - delete ", say, 1953." and substitute "1954."
21. Paragraph 5D3c(1) - insert "can be used only" between "attachment;" and "over".
22. Paragraph 5D3c(3) - delete "tactical" and substitute "tactical".
23. Paragraph 6 - amend to read as follows:
- "6. The Sub-Committee has the following recommendations to make:
- "a. That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this exploratory conference. This should include technical visits.

~~TOP SECRET~~

"b. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.

"c. That security evaluations be made and exchanged on all items discussed.

"d. That a copy of the final report of the conference be submitted to the U.S.-U.K. JCEC and that the U.S.-U.K. JCEC be requested to consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.

"e. That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time."

With respect to future meetings, MR. MILLER suggested that the Executive Committee meet after Sub-Committee "B" had made its second report so that if the working group had anything of interest to report, they could do so at that time. He added that it might be desirable to pass a copy of the conclusions to the COMINT Conference for their information. He pointed out that he saw no need for the Executive Committee to meet again until after the Sub-Committees had submitted their next reports, which would be sometime after 23 October 1950.

MR. FRIEDMAN inquired if there were any objections to Mr. Miller's suggestions.

There were none.

The meeting adjourned at 1625.

~~TOP SECRET~~

HEISA COMSEC CONFERENCE

AGENDA

Executive Committee Meeting, 1400, 11 October 1950

1. Approval of Minutes of 1st and 2nd Meetings.
2. Consideration of the Second Report of Subcommittee A.
3. Consideration of the Report of Subcommittee B.

~~TOP SECRET~~

~~TOP SECRET~~

FINAL

1

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE SECOND MEETING OF THE EXECUTIVE COMMITTEE

The Second Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1000 on 27 September 1950 in Room 17-318, U. S. Navy Security Station, Washington, D. C.

Representatives PresentUnited States

Mr. W. F. Friedman, Chairman
 Colonel S. P. Collins, USA
 Captain L. F. Safford, USN
 Captain J. S. Harper, USN
 Colonel R. C. Sears, USAF
 Lt. Colonel R. H. Horton, USA
 Lt. Colonel G. V. Johnson, USA
 Dr. A. Sinkov

United Kingdom

Captain, the Earl Cairns, R.N.
 Lt. Colonel C. A. Henn-Collins
 Commander J.R.G. Trechman, R.N.
 Brigadier John T. Tiltman

Secretariat

Lieutenant J. W. Pearson, U.S.N.
 Mr. H. D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~ITEM 1. CHAIRMANSHIP OF COMBINED EXECUTIVE COMMITTEE

MR. FRIEDMAN stated, for the record, that the Chairmanship for this particular meeting had been changed, by agreement, from Mr. Miller to himself.

ITEMS 2 AND 3 - BRITISH AND U. S. COMMENTS

MR. FRIEDMAN commented that the draft agenda which he had prepared was by no means all-inclusive, but would serve as a basis for discussion. He invited the members to bring up any additional matters which they wished to have considered. He then asked if any members of the British delegation wished to comment upon general progress of the Conference to date.

CAPTAIN, THE EARL CAIRNS expressed his opinion that things were going well indeed. He said that the completion of the Sub-Committee A assignment had taken rather longer than some had hoped; however, he thought the Sub-Committee had done a good job. He added that he would have additional comments when Item 5 of the Sub-Committee B assignment was considered.

MR. FRIEDMAN said that he thought Sub-Committee A was to be congratulated for having completed its work in such an expeditious manner. He referred to the minutes of the first meeting of the Executive Committee, stating that he had hoped to have them available for consideration at this meeting. He assured the members that copies would be distributed momentarily, and any proposed changes could be submitted at the next meeting.

ITEM 4. CONSIDERATION OF REPORT OF SUB-COMMITTEE A

With regard to the processing of final Conference papers MR. FRIEDMAN explained that the recommendations of the Conference would be subject to approval by higher authority on the U. S. side, in that it would be necessary to submit them to the U. S. Joint Chiefs of Staff via the Armed Forces Security Agency Council. He commented that this would take time but he thought it could be accomplished within one month.

COLONEL COLLINS agreed with this estimate, adding his presumption that the entire Conference report would be forwarded at one time.

CAPTAIN, THE EARL CAIRNS commented upon the large amount of work to be done by 1 January 1955, and said that the sooner a firm agreement could be reached the better.

~~TOP SECRET~~

~~TOP SECRET~~

COLONEL COLLINS said that it might be possible to forward the Conference recommendations in two separate parts, letting the Sub-Committee A recommendations be submitted in advance of the remainder of the Conference report.

CAPTAIN SAFFORD explained that the U. S. Joint Chiefs of Staff had already approved and submitted to the British the proposal for adoption of the 7-Rotor BCM. He said that upon British approval of the broad proposal, it would be necessary to obtain additional approval only on minor details.

MR. FRIEDMAN suggested that it might be well, then, to forward the Conference report in two separate parts.

COLONEL COLLINS agreed, explaining that the two separate matters had been combined only for convenience.

All members appeared to favor this procedure.

MR. FRIEDMAN then stated that, unless there was objection, it would be agreed that the report of Sub-Committee A would be handled as a separate matter and would be sent forward for approval immediately after the Combined Plenary Committee has reached final agreement with respect to it.

There was no objection to this decision.

MR. FRIEDMAN invited the members' attention to the report submitted by Sub-Committee A. He suggested that each member study it briefly before proceeding with a detailed consideration of it.

After a brief study the members considered the report in its entirety. As a result of this consideration it was agreed that the following changes would be made in the report as submitted by Sub-Committee A (Comments are included where appropriate):

1. Title - Change to read: "First Report of Sub-Committee A".
2. Paragraph 7, Line 3 - delete "Agreements", insert "recommendations". (Comment: It was agreed that the Sub-Committee could only recommend. Agreement will be sought from higher authority.)
3. Paragraph 7b - Change to read as follows: "Except by mutual agreement, disclosure of the 7-Rotor BCM principle will be limited to the U. S. and to the British Commonwealth. The British agree to notify the U. S. authorities when any issue of a combined 7-rotor BCM system is made to a nation of the British Commonwealth."

~~TOP SECRET~~

4. Paragraph 7e(7) - Change to read as follows: "And similar technical matters."
5. Paragraph 7e, final 3 sentences - Change to read as follows: "Upon completion of these studies the U. S. and the U. K. will exchange technical papers through established channels. If necessary, a special meeting to reconcile divergent views may be held in London (or Washington) at some later date."
6. Paragraph 7f, Line 2 - Change "Purposes" to "Purpose".
7. Paragraph 7f, Line 2 - Change "Agreement" to "Agreements".
8. Paragraph 7g, Line 3 - Delete "Given", insert "made available". (Comment: Change required for conformance to existing laws)
9. Paragraph 7h - Change to read as follows: "Make available to the British the tools and dies for MARK I rotors (for old TYPEX adapter)."
10. Paragraph 7i - Change to read as follows: "Make available to the British the tools and drawings of old TYPEX adapter, new design of TYPEX adapter rotors with tires, and parts and drawings for new TYPEX adapter."
11. Paragraph 8 - Change opening sentence to read as follows: "The following recommendations were agreed upon regarding improvement of security of present CCM until supersession date 1 January 1955 as proposed by the U. S. JCS in 2074/2 dated 27 December 1949."
12. Paragraph 8c - Change to read as follows: "Matters such as the rate of supersession and specific times of supersession are to be left to the established agencies charged with such matters."

MR. FRIEDMAN stated that the above changes would be written into the Sub-Committee A report and distribution would be made at an early date.

CAPTAIN HARPER asked if this report should be forwarded to the Plenary Committee at once, or held until the submission of the final report from Sub-Committee A.

CAPTAIN SAFFORD said that he would prefer to have it forwarded without delay.

All members agreed.

CAPTAIN SAFFORD departed from the meeting.

MR. FRIEDMAN asked if anyone wished to examine the retyped version of the report just considered, before it was forwarded to the Plenary Committee.

No one desired a re-examination, and MR. FRIEDMAN assured the members that every precaution would be taken to insure that the changes were correctly made. He added that copies would be distributed to all Committee members.

ITEM 5 - PLANNING FOR WORK OF SUB-COMMITTEE B

MR. FRIEDMAN asked Dr. Sinkov if he wished to comment on plans for Sub-Committee B.

DR. SINKOV replied that no concrete plans had been made, in anticipation of receiving general instructions from the Combined Executive Committee.

MR. FRIEDMAN asked Captain, the Earl Cairns if he had any particular desires with regard to the work of Sub-Committee B.

CAPTAIN, THE EARL CAIRNS suggested the possibility of having both morning and afternoon meetings.

MR. FRIEDMAN asked if this plan would be satisfactory with the U. S. members of Sub-Committee B who were pursuing their normal duties.

DR. SINKOV replied that it would depend largely upon how long the Sub-Committee continued to function.

COLONEL COLLINS suggested that no meetings be held on Saturday morning unless absolutely necessary.

DR. SINKOV proposed that the Sub-Committee meet every afternoon and two mornings per week.

CAPTAIN, THE EARL CAIRNS agreed with this proposal.

The members agreed to schedule the first three meetings for Wednesday afternoon, Thursday morning and Thursday afternoon-- additional meetings to be scheduled as a need for them was determined.

DR. SINKOV asked if Sub-Committee B should meet with the working groups concerned or meet as a Sub-Committee above and call in members of the working groups as necessary.

CAPTAIN HARPER said that it was contemplated that there would be simultaneous meetings of the working groups. He said that if such was not practicable it would be best to call the members in on an individual basis.

DR. SINKOV said that this procedure seemed best to him. He said he could have the American members of the working groups on call and available whenever they were needed.

MR. FRIEDMAN asked which item should be considered first.

DR. SINKOV said that the U. S. representatives were prepared to discuss the subject for Working Group No. 2.

CAPTAIN, THE EARL CAIRNS asked if were intended that the items would be considered in order of their listing.

MR. FRIEDMAN suggested that items "a" and "b" be consolidated.

CAPTAIN, THE EARL CAIRNS remarked that much work had been done on Item "a" and suggested that the two items be kept separate.

This suggestion was agreed to by all members.

DR. SINKOV then suggested that each item first be discussed generally on a broad basis, followed by a presentation of the U. S. and British views on the subject.

CAPTAIN HARPER asked that Sub-Committee B meet as soon as practicable to inspect a model of a small device, which it was necessary to return to the contractor at an early date for further development work.

LT. COLONEL HENN-COLLINS commented that his group had some devices which they wished to send back to England as soon as possible for the same reason. It was agreed that the Sub-Committee would meet at 1000, Thursday, 28 September 1950.

MR. FRIEDMAN stated that the time of the next meeting of the Combined Executive Committee was uncertain. He said that he would be away on Thursday and Friday but would return Monday. He would be willing to try to call a meeting on Monday afternoon, he said, if there was sufficient business for the Committee to consider.

It was agreed that the next meeting of the Combined Executive Committee would be held at the call of the Chairman.

The meeting adjourned at 1055.

29 September 1950

MEMORANDUM FOR THE MEMBERS OF THE EXECUTIVE COMMITTEE:

Subject: Tentative Minutes of the Second Meeting.

1. The subject minutes are forwarded herewith for your consideration.

2. Please advise the Secretariat, located in Room 19-211, U. S. Navy Security Station, (Telephone: Code 155, extension 353 or 354) of your comments and/or concurrence.

H. D. Jones
H. D. JONES
J. W. PEARSON
Secretariat

~~TOP SECRET~~BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE SECOND MEETING OF THE EXECUTIVE COMMITTEE

The Second Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1000 on 27 September 1950 in Room 17-318, U. S. Navy Security Station, Washington, D. C.

Representatives PresentUnited States

Mr. W. F. Friedman, ~~Acting~~ Chairman
 Colonel S. P. Collins, USA
 Captain L. F. Safford, USN
 Captain J. S. Harper, USN
 Colonel R. C. Sears, USAF
 Lt. Colonel R. H. Horton, USA
 Lt. Colonel G. V. Johnson, USA
 Dr. A. Sinkov

United Kingdom

Captain, the Earl Cairns, R.N.
 Lt. Colonel C. A. Henn-Collins
 Commander J.R.G. Trechman, R.N.
 Brigadier John T. Tiltman

Secretariat

Lieutenant J. W. Pearson, U.S.N.
 Mr. H. D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

ITEM 1. CHAIRMANSHIP OF COMBINED EXECUTIVE COMMITTEE

MR. FRIEDMAN stated, for the record, that the Chairmanship for this particular meeting had been changed, by agreement, from Mr. Miller to himself.

ITEMS 2 AND 3 - BRITISH AND U. S. COMMENTS

MR. FRIEDMAN commented that the draft agenda which he had prepared was by no means all-inclusive, but would serve as a basis for discussion. He invited the members to bring up any additional matters which they wished to have considered. He then asked if any members of the British delegation wished to comment upon general progress of the Conference to date.

CAPTAIN, THE EARL CAIRNS expressed his opinion that things were going well indeed. He said that the completion of the Sub-Committee A assignment had taken rather longer than some had hoped; however, he thought the Sub-Committee had done a good job. He added that he would have additional comments when Item 5 of the Sub-Committee B assignment was considered.

MR. FRIEDMAN said that he thought Sub-Committee A was to be congratulated for having completed its work in such an expeditious manner. He referred to the minutes of the first meeting of the Executive Committee, stating that he had hoped to have them available for consideration at this meeting. He assured the members that copies would be distributed momentarily, and any proposed changes could be submitted at the next meeting.

ITEM 4. CONSIDERATION OF REPORT OF SUB-COMMITTEE A

With regard to the processing of final Conference papers MR. FRIEDMAN explained that the recommendations of the Conference would be subject to approval by higher authority on the U. S. side, in that it would be necessary to submit them to the U. S. Joint Chiefs of Staff via the Armed Forces Security Agency Council. He commented that this would take time but he thought it could be accomplished within one month.

COLONEL COLLINS agreed with this estimate, adding his presumption that the entire Conference report would be forwarded at one time.

CAPTAIN, THE EARL CAIRNS commented upon the large amount of work to be done by 1 January 1955, and said that the sooner a firm agreement could be reached the better.

COLONEL COLLINS said that it might be possible to forward the Conference recommendations in two separate parts, letting the Sub-Committee A recommendations be submitted in advance of the remainder of the Conference report.

7. CAPTAIN SAFFORD explained that the U. S. Joint Chiefs of Staff had already approved and submitted to the British the proposal for transfer of the 7-Rotor BCM. He said that upon British approval of the broad proposal, it would be necessary to obtain additional approval only on minor details.

MR. FRIEDMAN suggested that it might be well, then, to forward the Conference report in two separate parts.

COLONEL COLLINS agreed, explaining that the two separate matters had been combined only for convenience.

All members appeared to favor this procedure.

MR. FRIEDMAN then stated that, unless there was objection, it would be agreed that the report of Sub-Committee A would be handled as a separate matter and would be sent forward for approval immediately after the Combined Plenary Committee has reached final agreement with respect to it.

There was no objection to this decision.

MR. FRIEDMAN invited the members' attention to the report submitted by Sub-Committee A. He suggested that each member study it briefly before proceeding with a detailed consideration of it.

After a brief study the members considered the report in its entirety. As a result of this consideration it was agreed that the following changes would be made in the report as submitted by Sub-Committee A (Comments are included where appropriate):

1. Title - Change to read: "First Report of Sub-Committee A".
2. Paragraph 7, Line 3 - delete "Agreements", insert "recommendations". (Comment: It was agreed that the Sub-Committee could only recommend. Agreement will be sought from higher authority.)
3. Paragraph 7b - Change to read as follows: "Except by mutual agreement, disclosure of the 7-Rotor BCM principle will be limited to the U. S. and to the British Commonwealth. The British agree to notify the U. S. authorities when any issue of a combined 7-rotor BCM system is made to a nation of the British Commonwealth."

4. Paragraph 7e(7) - Change to read as follows: "And similar technical matters."
5. Paragraph 7e, final 3 sentences - Change to read as follows: "Upon completion of these studies the U. S. and the U. K. will exchange technical papers through established channels. If necessary, a special meeting to reconcile divergent views may be held in London (or Washington) at some later date."
6. Paragraph 7f, Line 2 - Change "Purposes" to "Purpose".
7. Paragraph 7f, Line 2 - Change "Agreement" to "Agreements".
8. Paragraph 7g, Line 3 - Delete "Given", insert "made available". (Comment: Change required for conformance to existing laws)
9. Paragraph 7h - Change to read as follows: "Make available to the British the tools and dies for MARK I rotors (for old TYPEX adapter)."
10. Paragraph 7i - Change to read as follows: "Make available to the British the tools and drawings of old TYPEX adapter, new design of TYPEX adapter rotors with tires, and parts and drawings for new TYPEX adapter."
11. Paragraph 8 - Change opening sentence to read as follows: "The following recommendations were agreed upon regarding improvement of security of present CCM until supersession date 1 January 1955 as proposed by the U. S. JCS in 2074/2 dated 27 December 1949."
12. Paragraph 8c - Change to read as follows: "Matters such as the rate of supersession and specific times of supersession are to be left to the established agencies charged with such matters."

MR. FRIEDMAN stated that the above changes would be written into the Sub-Committee A report and distribution would be made at an early date.

CAPTAIN HARPER asked if this report should be forwarded to the Plenary Committee at once, or held until the submission of the final report from Sub-Committee A.

CAPTAIN SAFFORD said that he would prefer to have it forwarded without delay.

All members agreed.

CAPTAIN SAFFORD departed from the meeting.

MR. FRIEDMAN asked if anyone wished to examine the retyped version of the report just considered, before it was forwarded to the Plenary Committee.

No one desired a re-examination, and MR. FRIEDMAN assured the members that every precaution would be taken to insure that the changes were correctly made. He added that copies would be distributed to all Committee members.

ITEM 5 - PLANNING FOR WORK OF SUB-COMMITTEE B

MR. FRIEDMAN asked Dr. Sinkov if he wished to comment on plans for Sub-Committee B.

DR. SINKOV replied that no concrete plans had been made, in anticipation of receiving general instructions from the Combined Executive Committee.

MR. FRIEDMAN asked Captain, the Earl Cairns if he had any particular desires with regard to the work of Sub-Committee B.

CAPTAIN, THE EARL CAIRNS suggested the possibility of having both morning and afternoon meetings.

MR. FRIEDMAN asked if this plan would be satisfactory with the U. S. members of Sub-Committee B who were pursuing their normal duties.

DR. SINKOV replied that it would depend largely upon how long the Sub-Committee continued to function.

COLONEL COLLINS suggested that no meetings be held on Saturday morning unless absolutely necessary.

DR. SINKOV proposed that the Sub-Committee meet every afternoon and two mornings per week.

CAPTAIN, THE EARL CAIRNS agreed with this proposal.

The members agreed to schedule the first three meetings for Wednesday afternoon, Thursday morning and Thursday afternoon-- additional meetings to be scheduled as a need for them was determined.

DR. SINKOV asked if Sub-Committee B should meet with the working groups concerned or meet as a Sub-Committee above and call in members of the working groups as necessary.

CAPTAIN HARPER said that it was contemplated that there would be simultaneous meetings of the working groups. He said that if such was not practicable it would be best to call the members in on an individual basis.

DR. SINKOV said that this procedure seemed best to him. He said he could have the American members of the working groups on call and available whenever they were needed.

MR. FRIEDMAN asked which item should be considered first.

DR. SINKOV said that the U. S. representatives were prepared to discuss the subject for Working Group No. 2.

CAPTAIN, THE EARL CAIRNS asked if were intended that the items would be considered in order of their listing.

MR. FRIEDMAN suggested that items "a" and "b" be consolidated.

CAPTAIN, THE EARL CAIRNS remarked that much work had been done on Item "a" and suggested that the two items be kept separate.

This suggestion was agreed to by all members.

DR. SINKOV then suggested that each item first be discussed generally on a broad basis, followed by a presentation of the U. S. and British views on the subject.

CAPTAIN HARPER asked that Sub-Committee B meet as soon as practicable to inspect a model of a small device, which it was necessary to return to the contractor at an early date for further development work.

LT. COLONEL HENN-COLLINS commented that his group had some devices which they wished to send back to England as soon as possible for the same reason. It was agreed that the Sub-Committee would meet at 1000, Thursday, 28 September 1950.

MR. FRIEDMAN stated that the time of the next meeting of the Combined Executive Committee was uncertain. He said that he would be away on Thursday and Friday but would return Monday. He would be willing to try to call a meeting on Monday afternoon, he said, if there was sufficient business for the Committee to consider.

It was agreed that the next meeting of the Combined Executive Committee would be held at the call of the Chairman.

The meeting adjourned at 1055.

~~SECRET~~~~SECRET~~BRUSA COMSEC CONFERENCECombined Executive CommitteeMeeting on 27 September 1950AGENDA

1. Chairmanship of Combined Executive Committee.
2. Comments by British Mission.
3. Comments by U. S. Mission. *Statement & minutes
everything will have to be approved by
higher authority.*
4. Consideration of Report of Subcommittee A.
5. Planning for work of Subcommittee B.

~~SECRET~~

~~TOP SECRET~~

MR. MILLER inquired as to the arrangements for recording the proceedings of the Conference.

MR. FRIEDMAN replied that the Secretariat would publish the minutes of the Plenary and Executive Committee Meetings in summary form, but that verbatim minutes would not be taken, subject to the wishes of the British Delegation. He pointed out that, in time, recorders would be appointed for the Working Groups and the Sub-Committees. Turning to a new subject, he stated that office space had been provided for the British Delegation, and also spaces for the Working Groups. With regard to the meetings for the Sub-Committees, Mr. Friedman suggested that they be held daily in the afternoons starting on Monday, 25 September 1950, at one thirty or two o'clock, explaining that the U. S. Representatives were prepared to stay as long as necessary for the completion of business each afternoon.

MR. MILLER replied that one thirty o'clock was suitable to him.

MR. FRIEDMAN observed that it would be advantageous to keep the Meetings as small as is consistent with good workability, however, he emphasized that in event any Group or Committee Chairman deemed it desirable to call in technical assistance, he should feel free to do so. Turning to Mr. Miller, and making reference to the background statements that he had read at the First Meeting of the Plenary Committee, Mr. Friedman inquired if the British Delegation had any objections or comments to make particularly with regard to the articles quoted from the agreements.

MR. MILLER replied that his Delegation had no comments on the articles quoted from the agreements, but that they would like to make certain that they understood them.

MR. FRIEDMAN stated that he would make a copy available to the British Delegation for their study.

MR. MILLER recalled that a meeting of Sub-Committee A had been set for 0930 Friday morning, 22 September 1950, and inquired whether there would be a meeting in the afternoon.

CAPTAIN SAFFORD replied that the question of whether a meeting would be held in the afternoon would depend upon the progress of the morning meeting, and the wishes of the British Delegation. He emphasized that the U. S. Authorities did not wish to appear hasty in the premises, and invited the British to take as much time as they needed.

~~TOP SECRET~~

~~TOP SECRET~~

FINAL

1

BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FIRST MEETING OF THE EXECUTIVE COMMITTEE

The First Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1500 on 21 September 1950 in Room 1212, U. S. Navy Communication Station, Washington, D. C.

Representatives PresentUnited States

Mr. W. F. Friedman
 Colonel S. P. Collins, USA
 Captain L. F. Safford, USN
 Captain J. S. Harper, USN
 Colonel R. C. Sears, USAF
 Captain H. O. Hansen, USN
 Lt. Col. R. H. Horton, USA
 Dr. A. Sinkov

United Kingdom

Mr. T.R.W. Burton Miller, Chairman
 Captain, the Earl Cairns, R.N.
 Mr. Kenneth Perrin
 Mr. J.M.G. Pollard
 Lt. Col. C. A. Henn-Collins
 Mr. E. H. Jolley
 Brigadier J. H. Tiltman
 Group Captain Benjamin Ball, R.A.F.
 Commander J.R.G. Trechman, R.N.

Secretariat

Lieutenant J. W. Pearson, U.S.N.
 Mr. H. D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER stated that he was most anxious to get along with the proceedings, and inquired if it would expedite and simplify matters if he stated at this time that the British views were favorable to the acceptance of the seven rotor machine for combined use; he observed that he wasn't sure whether this would limit in any way the amount of demonstration necessary.

CAPTAIN SAFFORD replied that such information might simplify and streamline the whole procedure, adding that possibly the matter of adopting the seven rotor machine for combined use could be settled on Friday, September 22nd.

CAPTAIN HARPER said that to finish the matter in one day was, in his estimation, a very optimistic outlook.

Captain, the Earl CAIRNS observed that he thought the matter of replacement of the CCM might take three days.

COLONEL COLLINS pointed out that discussions of the rotor problems would probably result in complications which might take more time to resolve than had been anticipated.

On the other hand, MR. FRIEDMAN remarked that if Captain Safford's optimism were well founded, and the CCM business finished on Friday, then Sub-Committee B could meet on Saturday morning. He suggested that for the sake of the record it might be well if Mr. Miller could designate the British membership on Sub-Committee A at this time.

MR. MILLER replied that he would like the whole visiting British Delegation, and in addition Brigadier Tiltman from time to time, accredited as members of Sub-Committee A.

COMMANDER TRECHMAN remarked that he and Group Captain Ball were interested only if matters relative to the North Atlantic Treaty Organization were to be discussed.

CAPTAIN SAFFORD explained that he did not anticipate any such discussions since the U. S. representatives were not authorized to consider North Atlantic Treaty Organization matters.

MR. FRIEDMAN commented that Sub-Committee B members could be designated at a later date, but it was his understanding that Mr. Miller desired the whole of the visiting delegation accredited to the Plenary and the Executive Committees.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER replied in the affirmative; he stated that he understood the function of the Executive Committee was to hear the findings of the Sub-Committees.

MR. FRIEDMAN replied that such was correct, and that the Executive Committee would report to the Plenary Committee.

MR. MILLER stated that he then could reduce the membership on the Executive Committee considerably, that the British representation on that Committee would consist of himself and Captain, the Earl Cairns.

MR. FRIEDMAN suggested that Mr. Miller might name the Chairman of Sub-Committee B at this time if he so desired, pointing out that Admiral Stone desired Captain Safford to be the Chairman of Sub-Committee A.

MR. MILLER replied that he himself would chairmen Sub-Committee B.

MR. FRIEDMAN inquired whether Mr. Miller desired secretarial assistance for his office.

MR. MILLER replied in the negative, stating that most of the recording would be taken care of at the meetings.

MR. FRIEDMAN inquired of Mr. Miller as to when he expected his exhibits and drawings to arrive.

MR. MILLER replied that the next sailing of the Queen Mary was scheduled for September 21st, arriving in New York in about five days; and - allowing two days for the material to reach Washington, it should arrive on or about September 28th.

COLONEL COLLINS suggested to Mr. Miller that when he was ready to call a meeting of Sub-Committee B that he consult Dr. Sinkov who headed the U. S. representatives on the Committee.

MR. FRIEDMAN inquired if there were any items the British Delegation wished to add at this time.

MR. MILLER replied that he would like definitions of two or three of the items.

COLONEL COLLINS remarked that most of the present agenda was merely an amplification of the agenda that Mr. Miller had received.

~~TOP SECRET~~

~~TOP SECRET~~

MR. FRIEDMAN explained that the agenda that Mr. Miller had received didn't contain the CCM item and stated that the other change consisted of the shifting of what is now Item 2e from its previous position of 2a.

Referring to item I.A.1. of the Enclosure to the Agenda, MR. MILLER inquired as to whether a machine or function was meant. He said that he would like to have some idea as to the significance of the various categories.

MR. FRIEDMAN replied that a function was meant with regards to the item in question.

MR. MILLER then inquired as to how item I.B.2. differed from item I.A.1.

DR. SINKOV replied that I.A.1. was a general statement of purpose, while functional requirements in I.B.2. meant how the equipment would actually function.

MR. MILLER requested a clarification and distinction between items I.C.2. and I.D.

CAPTAIN SAFFORD replied that the distinction lay between the machine on the one hand, and the operator of the machine on the other.

Making reference to item 2.a. of the agenda, MR. MILLER inquired whether "telegraphic" was included to distinguish from "telephonic".

CAPTAIN SAFFORD replied that the word "telegraphic" was intended to mean - within the scope of Morse code telegraph.

MR. FRIEDMAN remarked that U. S. Authorities had considered combining items 2.a. and 2.b. into one Working Group, due to the fact that they were closely related.

DR. SINKOV explained that the reason for the separation of the two was that the Merchant Ship Problem had been considered important enough in itself to be considered separately.

MR. MILLER agreed that it might be confusing if both were considered together.

Making reference to Enclosure A to the Agenda, item III A., Description or Model Demonstration, MR. MILLER stated that this was one case in which they would be limited to descriptions only, but that his Delegation would be happy to describe the various undertakings presently in progress at home.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER inquired of Mr. Friedman as to how long in advance of meeting dates he would like pertinent papers circulated - he asked if 48 hours in advance would be satisfactory.

MR. FRIEDMAN replied that 48 hours in advance would be satisfactory.

MR. MILLER inquired if there were any other items to come before the Committee.

There were none.

The meeting adjourned at 1533.

~~TOP SECRET~~

~~TOP SECRET~~

27 September 1950

MEMORANDUM FOR THE MEMBERS OF THE EXECUTIVE COMMITTEE:

Subject: Tentative Minutes of the First Meeting.

1. The subject minutes are forwarded herewith for your consideration.
2. Please advise the Secretariat, located in Room 211, Building 19, U. S. Navy Security Station, telephone extension 354, of your comments and/or concurrence.



J. W. PEARSON
H. D. JONES
Secretariat

~~TOP SECRET~~

~~TOP SECRET~~BRITISH - UNITED STATES COMMUNICATIONS SECURITY CONFERENCEMINUTES OFTHE FIRST MEETING OF THE EXECUTIVE COMMITTEE

The First Meeting of the Executive Committee of the British - United States Communications Security Conference was held at 1500 on 21 September 1950 in Room 1212, U. S. Navy Communication Station, Washington, D. C.

Representatives PresentUnited States

Mr. W. F. Friedman
 Colonel S. P. Collins, USA
 Captain L. F. Safford, USN
 Captain J. S. Harper, USN
 Colonel R. C. Sears, USAF
 Captain H. O. Hansen, USN
 Lt. Col. R. H. Horton, USA
 Dr. A. Sinkov

United Kingdom

Mr. T.R.W. Burton Miller, Chairman
 Captain, the Earl Cairns, R.N.
 Mr. Kenneth Perrin
 Mr. J.M.G. Pollard
 Lt. Col. C. A. Henn-Collins
 Mr. E. H. Jolley
 Brigadier J. H. Tiltman
 Group Captain Benjamin Ball, R.A.F.
 Commander J.R.G. Trechman, R.N.

Secretariat

Lieutenant J. W. Pearson, U.S.N.
 Mr. H. D. Jones
 Miss Catherine M. Johnson

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER inquired as to the arrangements for recording the proceedings of the Conference.

MR. FRIEDMAN replied that the Secretariat would publish the minutes of the Plenary and Executive Committee Meetings in summary form, but that verbatim minutes would not be taken, subject to the wishes of the British Delegation. He pointed out that, in time, recorders would be appointed for the Working Groups and the Sub-Committees. Turning to a new subject, he stated that office space had been provided for the British Delegation, and also spaces for the Working Groups, with regard to the meetings for the Sub-Committees, Mr. Friedman suggested that they be held daily in the afternoons starting on Monday, 25 September 1950, at one thirty or two o'clock, explaining that the U. S. Representatives were prepared to stay as long as necessary for the completion of business each afternoon.

MR. MILLER replied that one thirty o'clock was suitable to him.

MR. FRIEDMAN observed that it would be advantageous to keep the Meetings as small as is consistent with good workability, however, he emphasized that in event any Group or Committee Chairman deemed it desirable to call in technical assistance, he should feel free to do so. Turning to Mr. Miller, and making reference to the background statements that he had read at the First Meeting of the Plenary Committee, Mr. Friedman inquired if the British Delegation had any objections or comments to make particularly with regard to the articles quoted from the agreements.

MR. MILLER replied that his Delegation had no comments on the articles quoted from the agreements, but that they would like to make certain that they understood them.

MR. FRIEDMAN stated that he would make a copy available to the British Delegation for their study.

MR. MILLER recalled that a meeting of Sub-Committee A had been set for 0930 Friday morning, 22 September 1950, and inquired whether there would be a meeting in the afternoon.

CAPTAIN SAFFORD replied that the question of whether a meeting would be held in the afternoon would depend upon the progress of the morning meeting, and the wishes of the British Delegation. He emphasized that the U. S. Authorities did not wish to appear hasty in the premises, and invited the British to take as much time as they needed.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER stated that he was most anxious to get along with the proceedings, and inquired if it would expedite and simplify matters if he stated at this time that the British views were favorable to the acceptance of the seven rotor machine for combined use; he observed that he wasn't sure whether this would limit in any way the amount of demonstration necessary.

CAPTAIN SAFFORD replied that such information might simplify and streamline the whole procedure, adding that possibly the matter of adopting the seven rotor machine for combined use could be settled on Friday, September 22nd.

CAPTAIN HARPER said that to finish the matter in one day was, in his estimation, a very optimistic outlook.

Captain, the Earl CAIRNS observed that he thought the matter of replacement of the CCM might take three days.

COLONEL COLLINS pointed out that discussions of the rotor problems would probably result in complications which might take more time to resolve than had been anticipated.

On the other hand, MR. FRIEDMAN remarked that if Captain Safford's optimism were well founded, and the CCM business finished on Friday, then Sub-Committee B could meet on Saturday morning. He suggested that for the sake of the record it might be well if Mr. Miller could designate the British membership on Sub-Committee A at this time.

MR. MILLER replied that he would like the whole visiting British Delegation, and in addition Brigadier Tiltman from time to time, accredited as members of Sub-Committee A.

COMMANDER TRECHMAN remarked that he and Group Captain Ball were interested only if matters relative to the North Atlantic Treaty Organization were to be discussed.

CAPTAIN SAFFORD explained that he did not anticipate any such discussions since the U. S. representatives were not authorized to consider North Atlantic Treaty Organization matters.

MR. FRIEDMAN commented that Sub-Committee B members could be designated at a later date, but it was his understanding that Mr. Miller desired the whole of the visiting delegation accredited to the Plenary and the Executive Committees.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER replied in the affirmative; he stated that he understood the function of the Executive Committee was to hear the findings of the Sub-Committees.

MR. FRIEDMAN replied that such was correct, and that the Executive Committee would report to the Plenary Committee.

MR. MILLER stated that he then could reduce the membership on the Executive Committee considerably, that the British representation on that Committee would consist of himself and Captain, the Earl Cairns.

MR. FRIEDMAN suggested that Mr. Miller might name the Chairman of Sub-Committee B at this time if he so desired, pointing out that Admiral Stone desired Captain Safford to be the Chairman of Sub-Committee A.

MR. MILLER replied that he himself would chairmen Sub-Committee B.

MR. FRIEDMAN inquired whether Mr. Miller desired secretarial assistance for his office.

MR. MILLER replied in the negative, stating that most of the recording would be taken care of at the meetings.

MR. FRIEDMAN inquired of Mr. Miller as to when he expected his exhibits and drawings to arrive.

MR. MILLER replied that the next sailing of the Queen Mary was scheduled for September 21st, arriving in New York in about five days; and - allowing two days for the material to reach Washington, it should arrive on or about September 28th.

COLONEL COLLINS suggested to Mr. Miller that when he was ready to call a meeting of Sub-Committee B that he consult Dr. Sinkov who headed the U. S. representatives on the Committee.

MR. FRIEDMAN inquired if there were any items the British Delegation wished to add at this time.

MR. MILLER replied that he would like definitions of two or three of the items.

COLONEL COLLINS remarked that most of the present agenda was merely an amplification of the agenda that Mr. Miller had received.

~~TOP SECRET~~

~~TOP SECRET~~

MR. FRIEDMAN explained that the agenda that Mr. Miller had received didn't contain the CCM item and stated that the other change consisted of the shifting of what is now Item 2e from its previous position of 2a.

Referring to item I.A.1. of the Enclosure to the Agenda, MR. MILLER inquired as to whether a machine or function was meant. He said that he would like to have some idea as to the significance of the various categories.

MR. FRIEDMAN replied that a function was meant with regards to the item in question.

MR. MILLER then inquired as to how item I.B.2. differed from item I.A.1.

DR. SINKOV replied that I.A.1. was a general statement of purpose, while functional requirements in I.B.2. meant how the equipment would actually function.

MR. MILLER requested a clarification and distinction between items I.C.2. and I.D.

CAPTAIN SAFFORD replied that the distinction lay between the machine on the one hand, and the operator of the machine on the other.

Making reference to item 2.a. of the agenda, MR. MILLER inquired whether "telegraphic" was included to distinguish from "telephonic".

CAPTAIN SAFFORD replied that the word "telegraphic" was intended to mean - within the scope of Morse code telegraph.

MR. FRIEDMAN remarked that U. S. Authorities had considered combining items 2.a. and 2.b. into one Working Group, due to the fact that they were closely related.

DR. SINKOV explained that the reason for the separation of the two was that the Merchant Ship Problem had been considered important enough in itself to be considered separately.

MR. MILLER agreed that it might be confusing if both were considered together.

Making reference to Enclosure A to the Agenda, item III A., Description or Model Demonstration, MR. MILLER stated that this was one case in which they would be limited to descriptions only, but that his Delegation would be happy to describe the various undertakings presently in progress at home.

~~TOP SECRET~~

~~TOP SECRET~~

MR. MILLER inquired of Mr. Friedman as to how long in advance of meeting dates he would like pertinent papers circulated - he asked if 48 hours in advance would be satisfactory.

MR. FRIEDMAN replied that 48 hours in advance would be satisfactory.

MR. MILLER inquired if there were any other items to come before the Committee.

There were none.

The meeting adjourned at 1533.

~~TOP SECRET~~

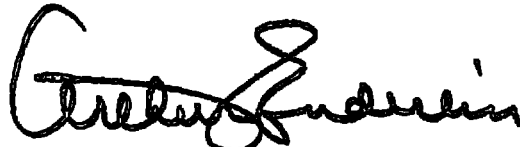
~~SECRET~~

COMSEC CONFERENCE
Working Group No. 1
17 October 1950

~~SECRET~~

Chairman's Memorandum No. 6

Working Group No. 1 met with combined subcommittee B on 17 October. The proceedings of the meeting will be recorded in the minutes of subcommittee B. The chairman of subcommittee B informed the chairman of working group No. 1 that the work of the latter group is completed, and that no formal report is required. If any further meetings of the group are required members of the group will be so advised.



Arthur Enderlin
Commander, USNR
Chairman.

cc: All members Working Group No. 1
AFSA-04T (Dr. Sinkov)
AFSA-12 (Col Horton)
AFSA-00T (Mr. Friedman)

~~SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

SECOND REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

Sub-Committee B resumed on 17 October after the arrival of Captain Hodges from Ottawa.

The second report of the Sub-Committee is attached hereto.

BRUSA COMSEC CONFERENCE

SECOND REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various cryptosystems falling in the general category of "Special purpose teleprinter systems for the exchange of communications intelligence material." The cryptosystems discussed are divided into the following groups:

	<u>NON-SYNCHRONOUS</u>		<u>SYNCHRONOUS</u>
	<u>ROTOR MAZE</u>	<u>KEY GENERATORS</u>	
U.S.	AFSAM-9	ASAM 2-1	AFSAM-9, if provided with synchronous features.
U.K.	- - -	Rollick	5 U.C.O. (Secrettype)

2. The AFSAM-9, ASAM 2-1 and Rollick are covered in the first report of Sub-Committee B. A description of the 5 U.C.O. is attached hereto.

3. The Sub-Committee has the following observations and conclusions to report on special purpose teleprinter systems for the exchange of communications intelligence material.

- a. We note that Rockex is presently being used for the exchange of communications intelligence material.
- b. We note that the 5 U.C.O. is in production and has been under test for the past six months, during part of this period between London and Ottawa.
- c. It is the British evaluation that the 5 U.C.O. is a true one-time system.
- d. It is the evaluation of the U.S. that the ASAM 2-1 with suitable one-time procedure, affords the necessary security for handling all classifications of traffic.
- 4. We conclude that:
 - a. If there is to be an immediate substitution for Rockex a selection can be made from the following machines:
 - ASAM 2-1
 - 5 U.C.O.
 - b. Either machine is available in sufficient quantity to meet current requirements in the exchange of communications intelligence material.

~~TOP SECRET~~

5. In the course of the discussions on equipments using one-time tapes, a brief description was given of British progress in key-tape production equipment. In view of the close association of such equipment with one-time systems, it is recommended that the subject of production equipment be added to the agenda of the next British-U.S. COMSEC conference.

~~TOP SECRET~~

~~TOP SECRET~~

~~SECRET~~~~SECRET~~Apparatus 5 U.C.O. Single Channel No. 1

On-line teleprinter cypher system.

Size and Weight

6' x 19" x 20"

500 pounds

Outline Description - Duplex on-line synchronous one-time teleprinter cypher system giving traffic flow security.

Technical Description

Cryptographic features - Cypher key is provided by continuously moving one-time 5 unit tapes. A spool of tape lasts about 4 hours.

Electrical features - Incoming teleprinter signals are stored and transmitted synchronously at 50 bauds after one-time element by element encypherment. The signals are regenerated before transmission to ensure perfect masking. The received signal is likewise regenerated. A full range of automatic alarms against potential insecurities is incorporated. For GCHQ operation special facilities are provided to secure exact one to one correlation between characters encyphered and decyphered (at the distant station). These facilities are for handling 32 character intercepts etc.

~~SECRET~~

~~TOP SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

SECOND REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

Sub-Committee B resumed on 17 October after the arrival of Captain Hodges from Ottawa.

The second report of the Sub-Committee is attached hereto.

~~TOP SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

SECOND REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various cryptosystems falling in the general category of "Special purpose teleprinter systems for the exchange of intelligence material." The cryptosystems discussed are divided into the following groups:

7 →

	NON-SYN ROTOR MAZE <u>NON-SYNCHRONOUS</u>	<u>KEY GENERATORS</u>	<u>SYNCHRONOUS</u>
U.S.	AFSAM-9	ASAM 2-1	AFSAM-9, if provided with synchronous features.
U.K.	- - -	Rollick	5 U.C.O. (Secrettype)

2. The AFSAM-9, ASAM 2-1 and Rollick are covered in the first report of Sub-Committee B. A description of the 5 U.C.O. is attached hereto.

3. The Sub-Committee has the following observations and conclusions to report on special purpose teleprinter systems for the exchange of intelligence material:

Commit

- a. We note that Rockex is presently being used for the exchange of intelligence material.
- b. We note that the 5 U.C.O. is in production and has been under test for the past six months, during part of this period between London and Ottawa.
- c. It is the British evaluation that the 5 U.C.O. is a true one-time system.
- d. It is the evaluation of the U.S. that the ASAM 2-1, with suitable one-time procedure, affords the necessary security for handling all classifications of traffic.

4. We conclude that:

- a. If there is to be an immediate substitution for Rockex a selection can be made from the following machines:

ASAM 2-1
5 U.C.O.

- b. Either machine is available in sufficient quantity to meet current requirements in the exchange of intelligence material.

7

~~TOP SECRET~~

~~TOP SECRET~~

5. In the course of the discussions on equipments using one-time tapes, a brief description was given of British progress in key-tape production equipment. In view of the close association of such equipment with one-time systems, it is recommended that the subject of production equipment be added to the agenda of the next conference. ^{British - US Communication Security}

~~TOP SECRET~~

~~SECRET~~~~SECRET~~Apparatus 5 U.C.O. Single Channel No. 1

On-line teleprinter cypher system.

Size and Weight

6' x 19" x 20"

500 pounds

Outline Description - Duplex on-line synchronous one-time teleprinter cypher system giving traffic flow security.

Technical Description

Cryptographic features - Cypher key is provided by continuously moving one-time 5 unit tapes. A spool of tape lasts about 4 hours.

Electrical features - Incoming teleprinter signals are stored and transmitted synchronously at 50 bauds after one-time element by element encypherment. The signals are regenerated before transmission to ensure perfect masking. The received signal is likewise regenerated. A full range of automatic alarms against potential insecurities is incorporated. For GCHQ operation special facilities are provided to secure exact one to one correlation between characters encyphered and decyphered (at the distant station). These facilities are for handling 32 character intercepts etc.

~~SECRET~~

~~TOP SECRET~~

Mr. Friedman

~~TOP SECRET~~

1
5
see 12
appendix

BRUSA COMSEC CONFERENCE

FIRST REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

The meetings of Sub-Committee B began on 27 September 1950 and continued intermittently through 13 October 1950.

The initial report of the Sub-Committee is attached hereto. The minutes that were kept of the meetings give only a summary of the highlights of the various subjects discussed. They are on file with the recorder.

~~TOP SECRET~~

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

13 October 1950

BRUSA COMSEC CONFERENCE

FIRST REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various crypto systems falling under the following item headings:

- a. Low Echelon (including Minor War Vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services.
- b. Merchant Ship Telegraphic Systems.
- c. Meteorological Security Systems, including Facsimile, Teleprinter and Telegraph.
- d. Voice Security Systems for Tactical Purposes.

2. During the course of the discussion and demonstrations 33 crypto systems were considered. Technical descriptions of 29 of these are included in the appendices as follows:

	<u>MACHINES</u>	<u>CIFAX</u>	<u>CIPHONY</u>	<u>HAND SYSTEMS</u>
U.S.	a. AFSAM 7 b. AFSAM 9 c. 7 Rotor BCM d. "PCM" e. MCM	f. ASAX 2 g. NRL Cifax	h. ASAY 4 i. ASAY 6 j. ASAY 8 k. AN/TRA 16 l. TSS	m. ASAD 1 n. Running Key Cipher
U.K.	o. Mercury p. Concert q. Rollick r. Singlet s. Pendragon t. DUP 1	s. METFAX	v. Hallmark w. Sorcerer x. D 70	y. Playfex z. Linex aa. Cursex bb. Otmetco cc. Alametco

Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries. Brief mention was made of a modification of the M-209 which has been proposed by Hagelin. A description which he has submitted is included in the appendix. The appendix also includes some miscellaneous notes on general items.

3. None of these crypto systems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations during the interim between the close of this conference and the opening of the next.

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~

4. Incidental to the discussions of the various crypto systems consideration was given to the problem of the number of different sizes of rotors which are contemplated for use in the mechanical crypto systems. The Sub-Committee feels that the 26-point rotor may have to be used for a long time to come but that some future agreement is necessary as to a selection among the 31, 32, and 36-point rotors. This agreement would limit the number of different types of rotors employed and thereby facilitate the interchangeability between U.K. and U.S. sources.

5. The Sub-Committee has the following observations and conclusions to report from its deliberation on the four items on its agenda:

A. Low Echelon (including Minor War Vessels) Telegraphic systems - including combined assault codes and tactical systems for all military Services.

1. We note that the Fleet Code and Combined Assault Codes are under discussion in the UK - US JC&C.

2. We note that there are no other Low Echelon systems yet under consideration for combined use.

3. We note that both US and UK have a number of new machine systems under development but that none of these is likely to be available for general combined use before 1954.

4. We conclude:

a. No machine system is likely to be available for general combined use before 1954.

b. If combined systems are required for any purpose in the interim period, possible systems are:

Strip
Linex
Cursex
Playfex
Running Key Cipher

c. To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months.

Possible devices are:

DUP 1
AFSAM 7
"PCM"
AFSAM 9
MCM
Concert
Rollick

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

B. Merchant Ship Telegraphic Systems.

1. We note that Cursex is under consideration in the US-UK JCEC and is likely to be adopted as the interim solution for Allied Merchant Ships.

2. We recommend that a machine system of at least equivalent security but faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

"PCM"
DUP 1
AFSAM 7
MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.

1. We note the lack of any suitable combined crypto system for meteorological purposes.

2. We note that both the UK and US have under development new meteorological systems in the following categories:

Air-Ground
Telegraph
Teleprinter
Cifax

3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for general combined use before 1954.

4. We note that requirements and characteristics for combined plain text facsimile equipments have not yet been agreed upon.

5. We conclude:

a. No machine crypto system for meteorological purposes is likely to be available for general combined use before 1954.

b. If combined systems are required for meteorological purposes in the interim period, possible devices are:

(1) Air-Ground - ASAD 1
Otmetco
Alametco

(2) Telegraph - CCM (modified for weather encipherment)
Pencil and paper system for very low echelon purposes.

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~

- (3) Teleprinter - ASAM 2-1
- (4) Facsimile - None available

c. To meet the long term requirements for encipherment of meteorological data selection should be made within the next 12 months.

Possible devices are:

- (1) Air-Ground - ASAD 1
 - Otmetco
 - Alametco
 - Any available ciphony system
- (2) Telegraph - BCM 7 with provision for weather encipherment
 - AFSAM 7
 - "PCM"
 - Singlet
 - Pendragon
 - DUP 1 - designed for weather encipherment
 - Pencil and paper systems
- (3) Teleprinter - AFSAM 9
 - ASAM 2-1
 - Concert
 - Kollick
 - Mercury
- (4) Cifax - ASAX 2
 - NRL Cifax
 - METFAX

NOTE: Selection in category (4) may not be possible until an agreement is reached in the UK-US JC&C on the requirements and characteristics for plain text facsimile equipments and associated transmission systems for meteorological use.

D. Voice Security Systems for Tactical Purposes.

1. We note that there are no ciphony systems under consideration for combined use.

2. We note that both the UK and the US have a number of new systems under development but that none of these is likely to be available for general combined use before 1954.

3. We conclude:

a. No ciphony system is likely to be available for general combined use before 1954.

b. There are no possibilities for suitable devices in the interim period.

c. To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. Possible devices are:

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

- (1) ASAY 4 (primarily designed as a low echelon ciphony attachment; can be used only over circuits of normal bandwidth)
- (2) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)
- (3) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)
- (4) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)
- (5) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)
- (6) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)

6. The Sub-Committee has the following recommendations to make:

- a. That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this exploratory conference. This should include technical visits.
- b. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.
- c. That security evaluations be made and exchanged on all items discussed;

~~TOP SECRET~~TOP⁵ SECRET

~~TOP SECRET~~~~TOP SECRET~~

d. That a copy of the final report of the conference be submitted to the U.S.-U.K. JCEC and that the U.S.-U.K. JCEC be requested to consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.

e. That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time.

~~TOP SECRET~~~~TOP SECRET~~

~~SECRET~~aAFSAM 7OFF-LINE PERMUTING CYPHER MACHINE FOR TACTICAL USE

Size 12" wide by 12" high by 6" deep, approximately, less case.
14" wide by 14" high by 8" deep, approximately, in case.

Weight 15 lbs less case; 22 lbs in case.

Outline Description - A keyboard operated, tape-printing cypher machine 24 v D.C. operated (with adaptor for 115 v - 230 v AC operation). Encyphers letters and figures.

Technical Description

Cryptographic features: Eight ³⁸/~~26~~-point rotors with independent alphabet and notch rings. 26 way input and output, 10 paths being re-entrant. Rotors 1-3, 5-8 turn. Motion is electrically controlled by sensing notch rings. Motion is "interlocked cascade," rotors 1 to 3 providing a dilated cyclometer giving a guaranteed minimum cycle. Machine is considered secure under all usual sorts of misuse. Read before step operation. Clear indicators are used.

Mechanical Features: A flying type wheel printer is used carrying a pulse generator on the same shaft. On depressing a key a circuit is set up through one stator coil in the pulse generator. At the appropriate time a pulse is generated in this coil which fires a thyatron operating the print magnet.

State of Progress - In an advanced state of development.

~~SECRET~~

~~SECRET~~~~SECRET~~

b

AFSAM 9ON-LINE 32 WAY PERMUTING CIPHER MACHINE FOR TELEPRINTER USE

Size 16" x 12" x 6" less case
18" x 14" x 8" with case

Weight Approximately 27 lbs less case
Approximately 35 lbs with case

Outline Description - A tactical high security teleprinter cipher machine accepting teleprinter signals as an input and producing teleprinter signals as an output. Employs start-stop synchronization.

Employment - For use wherever teleprinter is employed in tactical echelons. (Tactical use of teleprinters is planned on a broad scale as low as regiment or battalion).

Technical Description - Accepts an input teletype signal, stores the five intelligence bands, translates to one hot wire of 32, permuted in a rotor maze, the cipher signal translated to the five unit code for storage, and then transmitted in time sequence. Capable of operating at teleprinter speeds from 60 to 100 words per minute.

Cryptographic features - Employs nine 36-point rotors in the maze with 4 circuits reentered to reduce to a 32 character encipherment. Eight rotors move in an interlocked cascade with the center rotor not moving but fixed for the day. Three rotors automatically zeroized to a predetermined position before each message. Planned for use in a 5-letter clear text indicator with no restrictions as to use.

State of Progress - In advanced development. Prototype models expected Spring 1951.

~~SECRET~~

~~SECRET~~

8

7 ROTOR BCM (CSP 4800)

OFF-LINE 26-WAY PERMUTING MACHINE

Size 16" wide by 12" high by 12" deep, approximately

Weight 100 lbs approximately

Outline Description - 7 rotor mechanism using the carcass of CSP 1700 (CCM Mk II) with a single tape printer and a non-locking keyboard.

Technical Description -

Cryptographic Features: 7 rotor non-reciprocal maze. Planned to use removable notch rings and alphabet tyres. Rotors are reversible. Progression is notch controlled. Likely order of drive is 4 6 2 7 1 5 3, with 4 6 and 2 forming a cyclometer and the rest moving as in CCM. Rotors 2 and 6 always step backwards. Alteration of the direction of rotation of any rotor involves mechanical work. Maze is read before stepping. Backwards and forwards motion occur simultaneously.

Mechanical Features: Non-locking 4-bank keyboard with the numerals 1 to 0 on the top bank. Printer is magnet operated. 26-letter single case encypherment only. Printer has 26 letters, space and numerals 1 to 0 only. Facilities switch gives following conditions:

O - off

P - plain (in this condition all keys are effective)

D - decypher

E - encypher

R - reset (in this condition the rotors can be set by the figure keys 1 to 7)

Hand-drive facility of CSP 1700 has been abandoned, and the operation is by low voltage. An AC motor is fitted, and the printer, etc. is directly AC operated.

Another facility switch changes from CSP 4800 to CSP 1700. In the 1700 condition blank rotors are inserted in positions 2 and 6 (the backwards rotors) and these rotors will turn.

~~SECRET~~~~SECRET~~

c

7 ROTOR BCM (CSP 4800)OFF-LINE 26-WAY PERMUTING MACHINEMechanical Features: (Continued)

A variant of this machine for weather operation (i.e. net) was also shown. The weather switch connects the figures 1 to 0, space and X on encyphment to the maze, and on decyphment connects the appropriate maze outputs to the numerical functions of the printer.

As an alternative to this scheme the same facilities may be provided by using special plugs and sockets connected into the snakes joining the scrambler to the machine base.

Socket connections for auto operation are provided.

~~SECRET~~

~~SECRET~~~~SECRET~~d"PCM"

Size $\frac{1}{2}$ cubic foot - 12" x 12" x 6" approximately

Weight 15 pounds

Technical Description - This machine is cryptographically identical with the CSP 4800. The rotors, approximately $2\frac{1}{2}$ " in diameter will use removable notch rings and alphabet tires. Permits direct encryption of numerals.

State of Progress - Engineering model to be delivered about 15 November 1950.

~~SECRET~~

~~SECRET~~~~SECRET~~

e

CSP-3600 (MCM)OFF-LINE HAGELIN-TYPE CIPHER MACHINE

Size 10" wide by 10" high by 6" deep approximately.

Weight 12-16 lbs approximately.

Outline Description - Keyboard operated, tape-printing cipher machine intended for very low echelon use. Hand powered with provision for modification to motor drive.

Technical Description

Cryptographic Features: 12 M-209 pin wheels adding their combined effect to a common drum. Key is the result of two steps of the pin wheels. Pins and lugs are settable, with a maximum of 6 lugs to a bar.

State of Progress - In development with one preliminary engineering model available.

~~SECRET~~

~~SECRET~~~~SECRET~~fASAX 2CIFAX TRANSMITTER FOR USE WITH BLACK-WHITE COPY, PRIMARILY FOR WEATHER MAPS

Size 1 Rack approximately 24" x 26" x 54"
1 Power supply approximately 14" x 24" x 10"

Including approximately 150 vacuum tubes of which 130 are dual triodes.

Weight 400 lbs.

Outline Description - Medium-high echelon, high security cifax, transmitting multitone cipher at effectively 1000 elements per second, produced by synchronous binary addition of 2-level quantized facsimile signal and 2-level key.

Technical Description

Cryptotechnique: Six basic sequences produced at 6000 elements per second are combined in a complex manner to produce a 2-level key at 1000 elements per second. The basic sequences are produced by six continually rotating relatively prime wheels (in the range 101 to 115).

Electronic Features: The ASAX 2 is designed to transmit over 300-2750 cps land-line or HF radio, either or both being included in a single circuit. Cipher at a 1 millisecond rate is read successively into four channels, each channel being amplitude modulation of an audio subcarrier. A fifth subcarrier is amplitude modulated by a 50 cps signal for automatic phase control. The composite signal is transmitted directly on land-line or modulates a conventional (double sideband AM) HF radio transmitter.

The receiver portions of the ASAX 2 are equipped for automatic starting, synchronization, continuous phase correction, and alarming, including indication of each function. A frequency standard is included for use when manual control is desired.

State of Progress - Two terminals, originally designed for engineering tests, have gone through limited service testing on land-line and on HF radio links up to 1000 miles. Technically, performance of the equipment was satisfactory over normal ranges of room temperature.

~~SECRET~~

~~SECRET~~~~SECRET~~

E

NRL CIFAXCIFAX TRANSCEIVER FOR BLACK-WHITE WEATHER COPY

Can be converted to full duplex by addition of a second key generator.

Size Transmission equipment 16" x 19" x 72" approximately,
Key generator 16" x 19" x 24" approximately.

Weight 500 lbs approximately.

Outline Description - High security, shipboard and base station cifax, transmitting multitone cipher at effectively 1000 elements per second, produced by synchronous binary addition of a 2-level quantized facsimile signal and 2-level key.

Technical Description

Cryptotechnique: Eight basic sequences are reproduced at 1000 elements per second from continuously rotating wheels that are relatively prime. Eight wheels are selected from a set of 28 in the range 101 to 199. Four sequences are binary added to produce X key, which is recorded as a continuously traveling magnetic tape having 10 reading heads. A four stage ring picks off X key from various preselected reading heads to produce Y key. X key and Y key are binary added to produce the final output key. Two of the unused basic sequences are added Boolean to determine when the four stage ring is reset. The remaining two basic sequences determine to which position the ring is reset when a reset is demanded.

Electronic Features: The NRL cifax equipment transmits AM sub-carriers in the range 2000-3750 cps, eight channels being transmitted over Class A telephone line or HF single sideband radio. The equipment incorporates precision frequency standards with provision for manual or automatic phase correction.

State of Progress - Two models have received engineering tests and operate satisfactorily. Four service test models are presently being completed by a contractor.

~~SECRET~~

~~SECRET~~

h.

ASAY 4

TIME DELAY SCRAMBLE CIPHERY SYSTEM

Size 12" x 12" x 18", estimated.

Weight 15 pounds, estimated.

Outline Description - The individual elements within a group of 20 elements are delayed different amounts of time before transmission.

Technical Description - A 19 x 20 element matrix code box controls the delay of the specific elements of speech in each group of 20 elements. The same code is used for at least one conversation. The key code control is on a tape and is advanced one step to a new position. Whether change is to be on a message or time basis has not yet been established.

State of Progress - Engineering models are now under development.

~~SECRET~~~~SECRET~~

1

ASAY 6

Size Three bays approximately $5\frac{1}{2}$ x $2\frac{1}{2}$ x $1\frac{1}{2}$ feet.

Weight Approximately 250 pounds per bay plus spare parts and test equipment.

Technical Description - Speech is converted into a 1500 baud per second on-off signal by means of a vocoder and PCM coder. To this signal is added a key sequence from an associated key generator. Transmission is accomplished by eight frequency multiplexed channels located in the standard voice frequency band. Six of these channels are for speech information, one is for synchronization and one is for station selection. The receiving end accomplishes the reverse operations of the transmitting end. Each terminal is full duplex.

Cryptographic Features - The key generator makes use of the geared timing mechanism to produce six basic sequences of 101, 103, 107, 109, 113, and 115 elements length. These sequences are combined by addition and multiplication in electronic circuits to produce output key at 1500 elements per second. The basic patterns are changeable as well as the individual starting points of each sequence.

State of Progress - Three models of the equipment are under construction by a contractor. These will be engineering and service tested to determine necessary modifications.

~~SECRET~~

~~SECRET~~~~SECRET~~

1

ASAY 8SINGLE CHANNEL PCM CIPHER SYSTEM

Size 2 cases each 12" x 12" x 18" estimated.

Weight 50 lbs., estimated.

General - The system is intended for general airborne tactical usage by VHF radio.

Outline Description - A single channel PCM system which employs "push to talk" transceiver element scrambling of a block of 32 pulses.

Technical Description

Cryptographic Features: The PCM coder output is "flattened" by means of "auto key techniques." The least weight baud of each speech sample (4 digit PCM) is delayed multiples of five elements. This causes it to be added to the 8 weight bauds of the next sample, to the 4 weight bauds of the next sample after that, and the 2 weight baud of the next sample after that. A code card or rotor system is used to determine a transposition in a block of 32 elements.

State of Development - Early development. 2nd Engineering model to be built by contractor. Air transmission test planned on lab model.

~~SECRET~~

~~SECRET~~~~SECRET~~

k

AN/TRA-168 CHANNEL SPEECH SYSTEM FOR MICRO-WAVE RADIO

Size 7 4½ bays (counting 100% standby)

Weight About 1 ton (2000 lbs)

Outline Description - Enciphered PCM system transmitted by on-off pulses over micro-wave radio. The channels are in time division multiplex.

Technical Description

Cryptographic Features: The machine employs a key generator using four wheels of length 11, 13, 20, and 28. The motion of those wheels is controlled by plain text PCM elements and partially enciphered PCM elements.

State of Progress - Two terminals are nearing completion for use in a special experimental radio link. Several terminals without complete keyer circuits are available.

~~SECRET~~

~~SECRET~~~~SECRET~~1T.S.S.

Tactical speech encipherment system primarily for aircraft use.

Size and Weight - About 10" x 10" x 18" and weighs 39 pounds. (This is 18 element model.)

Outline Description - A TDS system of encipherment applied to PAM speech samples. Uses a fixed self-conversing code changeable by means of a switch matrix.

Technical Features - The set employs a rotary beam tube instead of a more conventional ring circuit to control the TDS operation. Two models of the system have been built, one employing a 12 element TDS the other an 18 element TDS. A 5 to 10 kc channel is required for transmission. The system synchronizes phase automatically.

State of Progress - Two models of each of the two types will soon be available for testing.

~~SECRET~~

~~SECRET~~~~SECRET~~IIASAD 1

1. ASAD 1 is a small hand substitution device, designed for use in multiseater aircraft for the transmission of essential meteorological information.

2. It consists of a black box about 12" x 7 $\frac{1}{4}$ " x 1 $\frac{1}{2}$ " in dimension, containing a letter key-roll which can be rotated horizontally and overlaid by a stencil which can be rotated vertically. The stencil contains 13 lines each designated by the type of information involved (e.g. cloud ceiling, visibility, etc.) and containing up to 20 holes designated by numbers, directions, etc. Thus, at any position of the stencil or key-roll, there are 13 lines showing different types of information, and the exact detail can be designated by the letter appearing in the appropriate hole on the line.

3. The key-roll is produced so that a letter never repeats within a series of 20. The stencil is designed so that it covers every other line and column of the key; there are thus four independent keys on the roll. The roll can be set in 100 positions and the stencil in 26 positions. The setting numbers are substituted into random digraphs by means of an indicator table which fits into a slot above the window of the device.

4. The cryptographic principle is similar to that of the British UCO or ALAMETCC, and the system can be used for transmitting the same kind of information. A wider choice of key is available owing to the length of the key-roll and the principle of dual slide.

~~SECRET~~

~~SECRET~~~~SECRET~~nRUNNING KEY CYPHER

1. RKC is a literal hand substitution cypher, designed to give a high degree of security on strategical links where machine systems are not available.

2. The cypher comprises a book of random literal key-groups, and a book of random 26 x 26 letter substitution squares, one for each day of the month. For point-to-point working, the keybook would be used "once through" each day, commencing at a point chosen at random in the table; the system can also be employed for group working, choosing a random starting-point for each individual message. The encryption process consists of substituting each plain-text letter in turn against its associated key-letter, employing the substitution table valid for the day.

~~SECRET~~

~~SECRET~~~~SECRET~~

9

MERCURY (LATE TYPEX Mk 10)

Synchronous on-line teleprinter cipher machine.

Size One 5'6" rack and four special tables.

Weight 450 lbs, very approximately

Outline Description - 31 way rotor permuting cipher machine using separate turnover control and ciphering mazes.

Technical Description

Cryptographic Features: A 4 rotor cyclometric maze controlling a 6 rotor ciphering maze. Rotors consist of an outer annulus (carrying progression notches) with scrambled wiring and a separate inner rotor. The two parts can be assembled in 62 different ways. Current traverses through the outer rotor section, then through a scrambled turn around end plate and then returns through the inner rotor sections. Cryptographically therefore the mazes consist of 9 and 13 rotors respectively.

Mechanical Features: Mercury is a duplex on-line synchronous cipher system. In-coming teleprinter signals are tried out to 31 ways and fed onto alternate storage devices. Signals are fed synchronously to the maze and then reconverted to 5 unit code for transmission. The maze is stepped synchronously. In the no traffic condition the letters function is sent "en clair" to line.

State of Progress - One circuit on traffic experimentally.

~~SECRET~~

~~SECRET~~~~SECRET~~

2

CONCERTON-LINE TELEPRINTER SYNCHRONOUS CIPHER MACHINE

Size 16" x 8" x 8" approximately.

Weight 40 lbs approximately.

Outline Description - A synchronous on-line subtractor teleprinter cipher machine for general tactical usage.

Usage - The device is planned for large scale tactical usage.

Technical Description

Cryptographic Features: Maze consists of 11 wired rotors periods 41, 43, 43, 45, 45, 46, 46, 47, 47, 49, 49. Rotors 1, 3, 5, 7, 9, 11 turn regularly one step per element. Rest stay still. 8 of the 49 paths through the maze "drop" off" at various points. 24 of 49 inputs are energized with battery through push-buttons and seven of the 41 outputs are tapped and fed into relays. The seven relays perform modulus 2 addition in series on the plain teleprinter element for encipherment. Rapid clearance of push-buttons is provided. Rotors not interchangeable; rotateable alphabet tyre. The device is capable of providing several streams of simultaneous key and will still be secure.

Mechanical Features: The maze turns, continuously driven, through a differential gear box for phasing purposes from a magnetic amplified controlled motor if high "Q" circuit is used for time control. Element storage is provided. Traffic is enciphered on an element by element basis including start and stop signals thereby giving traffic flow security.

State of Progress - Two lab models made from drawings are under test. Development of the time control features is incomplete.

~~SECRET~~

~~SECRET~~~~SECRET~~

2

ROLICKON-LINE TELEPRINTER CIPHER DEVICE

Size One 4'6" telegraph rack on castors

Weight 100 lbs approximately

Outline Description - An electronically operated half-duplex on-line teleprinter subtractor encipherment device.

Technical Description

Cryptographic Features: See notes on Cock-Robin. (Item ee).

The cipher key is generated by cold cathode gas tubes. Provision is made for generating random indicators not under control of the operator and for automatically positioning the key generator to these indicators.

Mechanical Features: The whole equipment is electronic. Most circuits use cold cathode gas tubes.

General - The device is intended initially for use on GCHQ land line circuits. A basic concept has been the use of electronic techniques so as to permit ready mass production.

State of Progress - Two models now being built for user trials.

~~SECRET~~

~~SECRET~~~~SECRET~~

2

SINGLET

General - Singlet is a keyboard operated motor-driven, tape-printing off-line permuting cipher machine. The keyboard corresponds exactly to a standard teleprinter keyboard except that there is one additional key called a "Bigram Key". The full range of teleprinter lower and upper case symbols are available but four letter keys and carriage-return and line-feed require the pre-operation of the bigram key.

The machine is designed to work from 100-125 volts or 200-250 volts 45-65 c/s single phase. It can be taken through the hatch of a submarine.

Details - The machine will have a 26-way maze with 7 or more rotors operating on BCM principles but can also be used as for CGM working. It will use American type rotors.

Use for Meteorological Traffic - The inclusion of full case-shift facilities enables the machine to be used for meteorological traffic. Since none of the bigrammed signals are used for this type of traffic the operation of the keyboard is exactly the same as that of a standard teleprinter. (Not a weather keyboard).

State of Progress - The machine is still under development. A development contract for prototype production models will probably be placed in the Summer of 1951.

~~SECRET~~

~~SECRET~~~~SECRET~~

1

PENDRAGON

General - Pendragon is an off-line cipher machine using a perforated tape input and producing a page-printed copy on a teleprinter and also, if required, a perforated tape on a printing reperforator.

The input tape can be prepared on a standard teleprinter perforator using the full range of teleprinter signals. Bigram signals are automatically inserted by the equipment which has a 26-way permuting maze exactly the same as that used in Singlet.

Pendragon will interwork with Singlet and can also be used for CCM or BCM working.

Details - The main unit will be identical with Singlet, except that the keyboard and printers will be replaced by a control unit for inserting carriage return and line-feed, etc.

State of Progress - Development is proceeding in parallel with the work on Singlet and it is expected that both Singlet and Pendragon will become available about the same time.

~~SECRET~~

~~SECRET~~~~SECRET~~

1

DUP 1

General - DUP 1 is an off-line hand operated tape-printing cipher machine with an electrical permuting maze, weighing about 18 lbs. Its dimensions are 12 $\frac{1}{4}$ " x 6 $\frac{1}{4}$ " x 5". On the model demonstrated, the input is controlled by a setting knob similar to that of M 209 but keyboard operation could be arranged. Electrical power is supplied by a self-contained 45 volt dry battery which gives 80,000 operations or more. For low temperature operation, an external source of power is necessary.

Details - The maze is 26-way and has 8 rotors of which 1 and 5 are fast turning, 2, 3 and 4 being driven cyclometrically by 1, and 6, 7 and 8 cyclometrically driven by 5.

The rotors have alphabet tyres rotatable with respect to turn-over patterns, and removable wiring inserts which can be fitted in any one of 26 positions. The turn-over pattern is the same on every rotor in a set and there are 16 wiring inserts to each set. Compromise of the machine and wirings is covered by the fact that adequate security is given in the daily setting.

Use for Meteorological Traffic - Proposals are under consideration for encipherment of numerals and the letter X by the use of a manually operated case shift.

State of Progress - One hand made model has been completed and six more are under construction. A development contract has been placed for the manufacture of 50 models engineered for large scale production and intended for Service trials. Delivery of these prototype production models is expected to commence during the Summer of 1951.

~~SECRET~~

~~SECRET~~~~SECRET~~

1

~~MET-FAX~~

General - MET-FAX is a system for the enciphered transmission of black and white meteorological charts. It is intended to meet a requirement for the transmission of charts 20" x 16" in a time of not more than 30 minutes with a definition of 100 lines per inch, the transmission channel (line or H.F.) having a band-width of 300 to 3,400 C/S.

The enciphering equipment will consist of one rack 20" wide by 6' high employing about 200 valves. The deciphering equipment is of about the same size.

According to present proposals the intelligence will be enciphered in an 8-way electrical permuting maze working entirely electronically.

Details:- The picture intelligence is quantized 4,500 times per second, that is at twice the nominal picture element rate so as to avoid degradation of definition. Groups of 3 quantized elements are converted to signals on one of eight wires having a recurrence rate of 1,500 per second. These signals are permuted and converted to signals having one of eight levels for transmission by F.M.

The permuter will have eight stages ("wheels") with pluggable turnover patterns and changeable wirings. The latter will consist of paxolin cards with metalized strip connections. The variables will be turnover pattern, order of progression and wiring. The deciphering equipment will be started automatically and its speed will be controlled by differentiation of the incoming signals.

Stage of Development - Back to back laboratory tests have been made using bread-board assemblies. Bread-board experiments of the transmission equipment are proceeding.

The electronic permuter may later be replaced by a Rollick key generator.

~~SECRET~~

HALLMARK

PCM CIPHERNY SYSTEM FOR TACTICAL USAGE

Size and Weight - Lab models consist of one 5'6" rack. Weight, 300 lbs approximately. Packaged equipment for vehicle use planned.

Outline Description - Duplex 32 level PCM subtractor encypherment ciphony system for point-to-point service.

Technical Description -

Cryptographic Features: Subtractor encypherment using binary key from a group of transition counters of moduli between 2 and 29. Counters are reset automatically by a maze at periodic intervals.

Technical Features: Duplex operation using a common key generator giving different key to go and return channels. Framing, synchronization, maze stepping, etc. is automatic.

State of Development - 6 copies of lab models being made for special GCHQ circuits. Development contract placed for engineered models for field use.

~~SECRET~~~~SECRET~~

II

SORCERERVOCODER SPEECH SECURITY SYSTEM FOR GENERAL USAGESize and Weight

(Planned) 2 double sided racks 5'6" high
600 lbs

Outline Description - PCM Vocoder analysis and synthesis system with subtractor encypherment for operation over circuits of normal bandwidth.

Technical Description

Cryptographic features: Encypherment will be by using the Cook-Robin principle.

Electrical features: One pitch and eight spectrum channels. Pitch channels are defined to 16 steps, the spectrum to 8 steps. Optional provision of two transmission systems, one for land line and VHF radio. Operating at 1800 bauds, and a multichannel V.F. system 170 cps spacing and a 100 baud speed on each channel. Provision can be made for a secure teleprinter channel for order wire purposes if required.

State of Development - Development contract placed with a contractor. First models for trial due in 18 months.

~~SECRET~~

~~SECRET~~~~SECRET~~xD 70MULTI-CHANNEL CENTIMETRIC RADIO RELAY EQUIPMENT

Size and Weight - Duplicate equipment consisting of 4 transmitters, 4 receivers, antenna masts, etc., carried in one vehicle. Duplicate PCM multiplex etc., carried in a second vehicle.

Outline Description - Centimetric radio relay system providing 12 top secret speech channels.

Technical Description

Cryptographic Features: Encypherment is carried out by the Cock-Robin principle (Item ee).

Electrical Features: The equipment is fully duplicated with automatic change-over facilities. The 12 PCM channels are carried by FM on a 6cm radio link. An engineering channel is also provided using the spectrum below 4 kc/s. PCM system is analogous to Hallmark.

~~SECRET~~

~~SECRET~~~~SECRET~~

Y

PLAYFEX (SMALL SHIPS CYFER)

1. Playfex is a tactical hand system, designed to effect a very rapid change of code with a minimum of documentation and production. It is specifically intended for use in small ships, and could be employed for any traffic where short term security is required and where a quick encryption process on a basic book is operationally acceptable.

2. In its present form it consists of a two-part (hatted) basic code-book, in which each vocabulary signification is given a two-letter group, omitting double letters and the letter J. The groups from the basic code-book are then encyphered by a double Playfair process, based on a pair of 5 x 5 squares changing every two hours. The keybook consists of 31 detachable pages, each containing 24 squares, divided into 12 pairs designated by the two-hour period for which they are valid. Each basic group is encrypted on the left hand square, and the resulting digraph encrypted on the right hand square. No indicator is required other than the date-time group of the message.

3. The keybook is designed so that squares valid for a period shorter than 24 hours can be issued for short front line operations. If a higher degree of security is required, the basic book can be changed monthly, the basic groups written out on a keylength, and the Playfair encryption applied to the vertical digraphs.

4. The small ships basic book and some editions of the keybook have been produced and are ready for issue if required. Field tests have proved satisfactory, but the system has not been used operationally.

~~SECRET~~

~~SECRET~~~~SECRET~~

2

LINEX

1. Linex is a literal hand substitution cypher, designed to give a high degree of security for forward-area strategical traffic, where machine systems are not available. It has been in use in the British Army forward of Brigade since 1944.

2. The cypher consists of a book of 25 pages of mixed alphabets, used in association with 10 cards known as cursors. Each cursor is designated by two or three letters, and contains a mixed alphabet along the top margin and a hole cut in one of ten positions on the right margin. The user selects one of the cursors and marks a letter in the mixed alphabet, as determined by the indicator. He finds the starting-point in the keybook, and places the marked letter under the first plain-text letter of the message; the cypher letter is read from the hole cut away on the right margin of the cursor. The cursor is then moved down one alphabet in the keybook and the process is repeated for the second plain-text letter; and so on, letter by letter through the message, using a new alphabet for each encryption.

3. The message indicator consists of a four-letter group selected from a page of random groups; the two pairs of letters are encrypted by a single Playfair process, to give the cursor and starting-point for the message.

~~SECRET~~

~~SECRET~~~~SECRET~~aaCURSEX

1. Cursex is a literal hand substitution cypher, designed to give a high degree of security for strategical traffic where machine systems are not available. It is specifically intended for use as a combined merchant ships' cypher, and would be suitable for use on strategical links or as a general back-up to machine systems.
2. The cypher consists of a book of literal key, used in association with a frame containing a horizontal- and a vertical- sliding keysheet made up of a number of mixed alphabets. The plain text is written under the groups in the keybook, starting at a point determined by the indicator, and each of the keysheets is set up at one of 26 positions in the frame. Each letter of the text is then encrypted on the alphabet indicated by the associated key-letter. The key-letter is found in the alphabet on the horizontal keysheet, and the substitution alphabet is taken from the vertical keysheet, the process being facilitated by the use of a cursor sliding vertically over the frame.
3. Several specimen frames and keysheets have been produced, and field tests have proved satisfactory.

~~SECRET~~

~~SECRET~~~~SECRET~~bbOTMETCO

1. Otmetco is a hand substitution cypher, designed for providing essential meteorological information to aircraft returning from operations. It can be used to transmit barometric pressure, followed by visibility and cloud-base if required. It is intended to place the minimum burden on the aircraft.
2. All ground-stations hold a book containing 1000 mixed alphabets, each designated by an indicator number. Aircraft are provided with a proforma card, containing an extract consisting of three alphabets from the book, a key barometric pressure and one or more letters indicating "plus" or "minus". The key pressure is obtained separately by each ground-station, by applying a daily-changing key-number to the actual barometric pressure observed at the station at a predetermined time.
3. When the aircraft returns to base, the ground-station transmits the barometric pressure as the deviation in millibars from the key pressure, in the form of a two-letter group; the first letter indicates "plus" or "minus", the second letter the deviation in millibars up to 25, as determined by the first alphabet on the card. If required, the cloud-base in hundreds of feet (up to 2500) is transmitted as the appropriate letter from the second alphabet, and the visibility in hundreds of yards (up to 2500) from the third alphabet.
4. In addition to the station key pressure, all aircraft in an area are given a daily-changing diversion key pressure. If an aircraft is diverted from base, it requests a report by transmitting its indicator number, and the ground-station bases its reply on the diversion key pressure.
5. Each indicator is allocated to one operation only, so that the key is virtually one-time, the only repetition being when a visibility or cloud-base alphabet on one operation may be used as a barometric alphabet on another.
6. The system is at present being given field tests, and preliminary indications are that it will prove satisfactory.

~~SECRET~~

~~SECRET~~~~SECRET~~CCALAMETCO

1. Alametco is a hand substitution cypher, designed for the transmission of meteorological information between ground-stations and aircraft. It has been in use in the R.A.F. since the latter part of the war.
2. Aircraft are provided with proforma cards, containing a number of lines devoted to various items of meteorological information, with blanks left for the insertion of letter keys (similar to the stencil on ASAD 1). Before an operation, the ground-station fills in the card with a number of mixed alphabets derived from a master key-book and changing daily. Any item can thus be expressed as the line-number in the proforma followed by the letter appearing in the appropriate space. Each aircraft normally carries more than one card, a different series being employed for area broadcasts.

~~SECRET~~

~~SECRET~~~~SECRET~~ddROTORS26-Point Rotors

It has been agreed on Sub-Committee A that rotors on both U.S. and British revisions of the 7-rotor BCM should be physically and cryptographically interchangeable. The size of rotor proposed (3½" diameter) is that now used on CSP 1700. It is also proposed that the physical design shall as and when possible take the form of a rotor with a soldered-in wiring bobbin, a removable turnover cam, and a removable alphabet tyre each of which are in effect capable of rotation. The rotors may be reversed by interchanging the position of the turnover cam and the alphabet tyre.

For lightweight machines it has been proposed that a rotor of similar design but having a diameter of 2½" (as used on PCM) should be employed.

31 Point Rotors (U.K.)

A 31 point rotor of special design is used in Mercury (British on-line teleprinter permuting system).

The rotor consists of an outer reversible scramble-wired annulus with a fixed turnover pattern and fixed alphabet tyre, in which is inserted a second scramble-wired disc. The insert may be fitted in any one of 31 positions and is reversible. The maze circuits first pass through the inserts and then return via the end plate through the annuli.

36 Point Rotors (U.S.)

The U.S. is developing a 36 point rotor for use in new cipher machine developments. The figure 36 was chosen to allow encipherment of the 32 character teletype alphabet, the 26 character literal alphabet, and various system wirings. Two physically identical types of rotors are being developed; one of whose wiring is capable of being "plugged" to any desired scramble, and a second whose scramble wiring is "printed" on a replaceable plastic insert.

Each rotor consists of 4 parts, a main body, a notch ring, an alphabet ring, and a lock ring. The main body contains 36 flush commutator contacts on one face and 36 plungers on the other face. The notch ring is interchangeable between rotors and, although it is not reversible, can be placed in 36 different positions with respect to the alphabet ring. The notch ring

~~SECRET~~

~~SECRET~~~~SECRET~~

dd - Rotors (continued)

provides stepping control for the maze. The alphabet ring is used as a drive ring and for message indicator settings and contains 10 blanks on its periphery. Opposite the letter "O" is a depression used to "zeroize" the rotor. The lock ring holds the assembly together. The daily set up will consist of assembling the alphabet ring in the proper juxtaposition to the main body's index mark, picking the proper notch ring and placing it in proper juxtaposition to the alphabet ring and locking the assembly by means of the lock ring.

The design goal was to produce a new rotor which would ease the rotor wiring problem and be capable of large scale production.

The dimensions are 3.7" OD, 0.42" thick, and a hub bore of 0.30". The expected normal life is over 200,000,000 operations.

~~SECRET~~

~~SECRET~~

ee

COCK-ROBIN

1. Note: Cock-Robin is a basic cryptographic principle, and has many applications. It can be produced both electronically and mechanically. It is described here in one application as a key generator (Rollick) for on-line teleprinter encipherment but other applications are mentioned in descriptions of devices using it.
2. Components: The generator has 9 cold cathode decade counters divided into three sets A, B and C. Each set has one counter 10, one 9 and one 7. All three counters within a set are driven simultaneously by means of an on/off gate. Several of the cathodes in each set are tapped, strapped together, and led off to control the other two gates. Another selection, possibly overlapping, of the cathode is made to produce three streams of mark/space key X, Y & Z, which are added modulo 2 to produce the final key element.
3. Motion: The "motor" output of set A turns Gate B on if there is a voltage present, and turns Gate C on if there is no voltage present. Set B controls Gate C and A, and Set C controls A and B in the same way. A gate is therefore only off if there is no voltage from the preceding set and there is a voltage from the following set. When the number of tappings in the various sets satisfy a certain condition, the cycle is the guaranteed maximum of $10 \times 9 \times 7$ cubed.
4. Key: Stream X is obtained by tappings from the 10 counters in Set A, the 9 in B and the 7 in C, these tappings being strapped to give Boolean addition. Y is obtained from the 10 in B, the 9 in C and the 7 in A, and Z from the 10 in C, the 9 in A and the 7 in B. X, Y and Z are then added modulo 2 for the final key element, which is added to the plain teleprinter element.
5. Settings: All the tappings of cathodes for key and motorization are completely pluggable, and obviously change of plugging, which will probably be daily, gives a change of machine. Message settings can generally be produced automatically (see description of Rollick).

~~SECRET~~

~~SECRET~~~~SECRET~~

ff

CIPHONY SCHEME FOR GROUP WORKINGOutline Description of Proposal

A scheme for quantising speech into say 8 levels and permitting these levels in both electronic and mechanical (maze) permitters. Synchronization of the electronic circuits can be achieved on a push-to-talk basis, the mechanical parts by a clock mechanism. In this manner the advantages of permutation can be used in mitigation of loss of security due to transmission in depth.

~~SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

FIRST REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

The meetings of Sub-Committee B began on 27 September 1950 and continued intermittently through 10 October.

The final report of the Sub-Committee is attached hereto. The minutes that were kept of the meetings give only a summary of the highlights of the various subjects discussed. They are on file with the recorder.

~~TOP SECRET~~

~~TOP SECRET~~

~~TOP SECRET~~

10 October 1950

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various crypto systems falling under the following item headings:

- a. Low Echelon (Minor War Vessels) Telegraphic Systems - ^{including} including combined assault codes and tactical systems for all military Services.
- b. Merchant Ship Telegraphic Systems.
- c. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.
- d. Voice Security Systems for Tactical Purposes.

2. During the course of the discussion and demonstrations 31 crypto systems were considered. Technical descriptions of 27 of these are included in the appendices as follows:

- a. AFSAM 9
- b. Mercury
- c. Concert
- d. Rollick
- e. AFSAM 7
- f. "PCM"
- g. Singlet
- h. Pendragon
- i. DUP 1
- j. MCM
- k. 7 rotor ECM
- l. ASAX 2
- m. NRL Cifax
- n. METFAX
- o. ASAY 4
- p. ASAY 8
- q. Hallmark
- r. Sorcerer
- s. D 70
- t. AN/TRA 16
- u. Playfex
- v. Linex
- w. Cursex
- x. ASAD 1
- y. Otmetco
- z. Alamstco
- aa. Running Key Cipher

Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries.

3. None of these crypto systems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations ~~on each side~~ during the interim between the close of this ^{Conf} session and the opening of the next.

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

4. Incidental to the discussions of the various crypto systems consideration was given to the problem of the number of different sizes of rotors which are contemplated for use in the mechanical crypto systems. The Sub-Committee feels that the 26-point rotor may have to be used for a long time to come but that some future agreement is necessary as to a selection among the 31, 32, and 36-point rotors.

5. The Sub-Committee has the following observations and conclusions to report from its deliberations on the four items on its agenda:

A. Low Echelon (^{including} Minor War Vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services.

1. We note that the Fleet Code and Combined Assault Codes are under discussion in the UK - US JCRC.

2. We note that there are no other Low Echelon systems yet under consideration for combined use.

3. We note that both US and UK have a number of new machine systems under development but ~~it is unlikely that any of these could be available for general combined use before 1954.~~ ^{that none of these is likely to be} ~~generally introduced in quantity for combined use before 1953.~~

4. We conclude:

a. No machine system is likely to be available for general combined use before ¹⁹⁵⁴ ~~1953~~.

b. If combined systems are required for any purpose in the interim period, possible ^{systems} ~~devices~~ are:

Strip
Linx
Cursex
Playfex
Running Key Cipher

c. To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months.

Possible devices are:

DUP 1
AFSAM 7
"PCM"
AFSAM 9
MCM
Concert
Rollick

B. Merchant Ship Telegraphic Systems.

1. We note that Cursex is under consideration in the US-UK JCRC and is likely to be adopted as the interim solution for Allied Merchant Ships.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~*of at least equal security but*

2. We recommend that a machine system faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

W PCM 11
DUP 1
AFS-M 7
MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.

1. We note the lack of any suitable combined crypto system for meteorological purposes.

2. We note that both the UK and US have under development new meteorological systems in the following categories:

Air-Ground
Telegraph
Teleprinter
Cifax

3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for ~~introduction into general combined use before, say, 1953.~~ ^{1954.}

4. We note that requirements and characteristics for combined plain text facsimile equipments have not yet been agreed upon.

5. We conclude:

a. No machine crypto system for meteorological purposes is likely to be available for general combined use before, ^{1954.} ~~say, 1953.~~

b. If combined systems are required for meteorological purposes in the interim period, possible devices are:

- (1) Air-Ground - ASAD 1
Otmeco
Alametco
- (2) Telegraph - CCM (modified for weather encipherment)
very
+ Pencil and pencil systems for low security purposes.
- (3) Teleprinter - ASAM 2-1 ~~(as described under item 2)~~
- (4) Facsimile - None available

c. To meet the long term requirements for encipherment of meteorological data selection should be made within the next 12 months.

Possible devices are:

- (1) Air-Ground - ASAD 1
Otmeco
Alametco
Any available ciphony system

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

- (2) Telegraph - BCM 7 with provision for weather encipherment
 AFSAM 7
 PGM 11
 Singlet
 Pendragon
 DUP 1 - designed for weather encipherment
Pencil and paper systems
- (3) Teleprinter - AFSAM 9
 ASAM 2-1
 Concert
 Rollick
 Mercury
- (4) Cifax - ASAX 2
 NRL FAX CIFAX
 MET FAX 2

(4)
 NOTE: Selection in ~~these~~ category may not be possible until an agreement is reached in the UK-US JCEC on the requirements and characteristics for plain text facsimile equipments and associated transmission systems for meteorological use.

D. Voice Security Systems for Tactical Purposes.

1. We note that there are no ciphony systems under consideration for combined use.

2. We note that both the UK and the US have a number of new systems under development but *that none of these is likely to be available for general combined use before 1954.* ~~it is unlikely that any of these could be generally introduced in quantity for combined use before, say, 1953.~~

3. We conclude:

a. No ciphony system is likely to be available for general combined use before ~~say, 1953.~~ *1954.*

b. There are no possibilities for suitable devices in the interim period.

c. To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. Possible devices are:

- (1) ASAY 4 (primarily designed as a low echelon ciphony attachment; *can be used only* over circuits of normal bandwidth)
- (2) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)
- (3) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

- (4) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)
- (5) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)
- (6) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)

6. The Sub-Committee has the following general recommendations to make:

- a. That ~~immediately and on a continuing basis there will be~~ a

complete interchange of the technical details of the systems discussed in ~~these~~ ^{this} exploratory conference. This should include technical visits.

b. That security evaluations be made and exchanged on all items discussed.

a copy of the final report of the Conference be submitted to the

c. That ~~the~~ U.S.-U.K. JCEC ~~be invited to consider and resolve, without as a~~ *so that it may* ~~delay~~ the operational requirements in all fields of Combined Cryptographic

Communications.

the next d. That ~~a~~ ^{the next} further conference be held in about nine months ^{in London} to arrive at final selections of items to be recommended for combined adoption *and that*

e. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.

on these subjects for
the next four years, to be
held alternately in London
and Washington, the first
of these to take place in London
in approximately nine months
time.

the next
alternately in
Washington and London.
additional conferences
be held

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

REPORT OF SUB-COMMITTEE B TO THE EXECUTIVE COMMITTEE

1. Sub-Committee B has made an exchange of technical information concerning various crypto systems falling under the following item headings:

- a. Low Echelon (Minor War Vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services.
- b. Merchant Ship Telegraphic Systems.
- c. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.
- d. Voice Security Systems for Tactical Purposes.

2. During the course of the discussion and demonstrations 31 crypto systems were considered. Technical descriptions of 27 of these are included in the appendices as follows:

- a. AFSAM 9
- b. Mercury
- c. Concert
- d. Rollick
- e. AFSAM 7
- f. PCM
- g. Singlet
- h. Pendragon
- i. DUP 1
- j. MCM
- k. 7 rotor ECM
- l. ASAX 2
- m. NRL Cifax
- n. METFAX
- o. ASAY 4
- p. ASAY 8
- q. Hallmark
- r. Sorcerer
- s. D 70
- t. AN/TRA 16
- u. Playfex
- v. Linex
- w. Cursex
- x. ASAD 1
- y. Otmetco
- z. Alametco
- aa. Running Key Cipher

Four others, the ASAM 2-1, the CCM, the Strip Cipher, and the M-209, have no descriptions attached because of their familiar status in both countries.

3. None of these crypto systems was subjected to serious deliberation as far as security is concerned and on many of them no security studies have yet been made. It is the aim of the Sub-Committee that these systems shall all receive security evaluations on each side during the interim between the close of this session and the opening of the next.

4. Incidental to the discussions of the various crypto systems consideration was given to the problem of the number of different sizes of rotors which are contemplated for use in the mechanical crypto systems. The Sub-Committee feels that the 26-point rotor may have to be used for a long time to come but that some future agreement is necessary as to a selection among the 31, 32, and 36-point rotors.

5. The Sub-Committee has the following observations and conclusions to report from its deliberations on the four items on its agenda:

A. Low Echelon (Minor War Vessels) Telegraphic Systems - including combined assault codes and tactical systems for all military Services.

1. We note that the Fleet Code and Combined Assault Codes are under discussion in the UK - US JCEC.

2. We note that there are no other Low Echelon systems yet under consideration for combined use.

3. We note that both US and UK have a number of new machine systems under development but it is unlikely that any of these could be generally introduced in quantity for combined use before, say, 1953.

4. We conclude:

a. No machine system is likely to be available for general combined use before, say, 1953.

b. If combined systems are required for any purpose in the interim period, possible devices are:

- Strip
- Linex
- Cursex.
- Playfex
- Running Key Cipher

c. To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months.

Possible devices are:

- DUP 1
- AFSAM 7
- PCM
- AFSAM 9
- MCM
- Concert
- Rollick

B. Merchant Ship Telegraphic Systems.

1. We note that Cursex is under consideration in the US-UK JCEC and is likely to be adopted as the interim solution for Allied Merchant Ships.

2. We recommend that a machine system faster than Cursex should replace it, when available, and that such a system should be selected within the next 12 months. Possible devices are:

PCM
DUP 1
AFSAM 7
MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph.

1. We note the lack of any suitable combined crypto system for meteorological purposes.

2. We note that both the UK and US have under development new meteorological systems in the following categories:

Air-Ground
Telegraph
Teleprinter
Cifax

3. We note that with the exception of the Air-Ground systems none of the systems under development is likely to be available for introduction into general combined use before, say, 1953.

4. We note that requirements and characteristics for combined plain text facsimile equipments have not yet been agreed upon.

5. We conclude:

a. No machine crypto system for meteorological purposes is likely to be available for general combined use before, say, 1953.

b. If combined systems are required for meteorological purposes in the interim period, possible devices are:

- (1) Air-Ground - ASAD 1
Otmotco
Alametco
- (2) Telegraph - CCM (modified for weather encipherment)
- (3) Teleprinter - ASAM 2-1 (to be described under Item E)
- (4) Facsimile - None available

c. To meet the long term requirements for encipherment of meteorological data selection should be made within the next 12 months.

Possible devices are:

- (1) Air-Ground - ASAD 1
Otmotco
Alametco
Any available ciphony system

~~TOP SECRET~~~~TOP SECRET~~

- (2) Telegraph - BCM 7 with provision for weather encipherment
 AFSAM 7
 PCM
 Singlet
 Pendragon
 DUP 1 - designed for weather encipherment
- (3) Teleprinter - AFSAM 9
 ASAM 2-1
 Concert
 Rollick
 Mercury
- (4) Cifax - ASAX 2
 NRL FAX
 MET FAX

NOTE: Selection in this category may not be possible until an agreement is reached in the UK-US JCEC on the requirements and characteristics for plain text facsimile equipments and associated transmission systems for meteorological use.

D. Voice Security Systems for Tactical Purposes.

1. We note that there are no ciphony systems under consideration for combined use.

2. We note that both the UK and the US have a number of new systems under development but it is unlikely that any of these could be generally introduced in quantity for combined use before, say, 1953.

3. We conclude:

a. No ciphony system is likely to be available for general combined use before, say, 1953.

b. There are no possibilities for suitable devices in the interim period.

c. To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. Possible devices are:

- (1) ASAY 4 (primarily designed as a low echelon ciphony attachment; over circuits of normal bandwidth)
- (2) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)
- (3) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET~~

- (4) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)
- (5) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)
- (6) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)

6. The Sub-Committee has the following general recommendations to make:
- a. That immediately and on a continuing basis there will be a complete interchange of the technical details of the systems discussed in these exploratory conferences. This should include technical visits.
 - b. That security evaluations be made and exchanged on all items discussed.
 - c. That the U.S.-U.K. JCEC be invited to consider and resolve without delay the operational requirements in all fields of Combined Cryptographic Communications.
 - d. That a further conference be held in about nine months to arrive at final selections of items to be recommended for combined adoption.
 - e. That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.

~~TOP SECRET~~~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

Third Report of Subcommittee A

24 October 1950

Sub
Comm
A

1. As recorded in the second report of Subcommittee A, this Subcommittee was reconvened on 23 October 1950 to consider the matter of encrypting letters plus numerals plus certain other Teleprinter characters, using the 7-rotor BCM crypto technique.
2. Subcommittee A has already recommended that the present CCM be replaced by the 7-rotor BCM crypto principle not later than 1 January 1955.
3. This replacement can be effected by both nations by modifying existing equipment and/or by introducing new equipment.
4. With the introduction of the new BCM crypto principle, the following operating facilities will be available:
 - (a) Texts consisting either of 26 letters plus space but not including numerals, or, alternatively, of 10 numerals plus one additional symbol plus space but not including letters, may be encrypted. On decryption "Z" will print as "X" as with the present CCM.
 - (b) None of the additional facilities, for example, a mixture of letters and figures, offered by a standard Teleprinter will be available.
5. The U.S. and the British are currently building new off-line cypher machines capable of employing the 7-rotor BCM principle and offering some or all of the facilities inherent in standard Teleprinters. The techniques by which these facilities will be provided is different in the U.S. design from that employed in the British design, due to differences in operating requirements, as set forth in paragraphs 7 and 8, below.
6. Both nations are agreed that the following general requirements, if possible, be met:
 - (a) Size and weight of the machine must show a marked reduction compared with existing machines.
 - (b) Encryption must be automatic to the greatest possible extent and to the lowest possible echelon.
 - (c) Mechanical and cryptographic deficiencies found in the CCM and earlier machines must be eliminated. Greater reliability

~~TOP SECRET~~

and simpler maintenance and adjustment must also be provided.

(d) Essential Teleprinter facilities must be provided.

It is in the interpretation of this last requirement that the U.S. and British views are at variance.

7. The British Operational Staff require that off-line machines which are to provide automatic encryption and decryption shall be capable of:

- (a) Accepting a tape, perforated on any Teleprinter employing the International Telegraph Alphabet No. 2. (See page 265, Telegraph Regulations, Cairo Revision of 1938)
- (b) Presenting automatically in page form the decrypted version identical with the original text. Thus, for example, all the Teleprinter functions required for tabulation which appeared in the original text must be reproduced during decryption and be capable of operating a standard Teleprinter.

8. The U.S. operational requirement has not been so exactly specified. The term "Essential Teleprinter Facilities" has been employed and is currently interpreted by the designers as requiring that the machine must be capable of receiving a Plain Language Tape perforated on any standard Teleprinter and must produce the decrypted version in page form. To provide these facilities the U.S. designers:

- (a) Use some but not all of the upper case characters. (Numbers and slant-mark are used)
- (b) Insert "Carriage Return" and "Line Feed" during decryption only at the end of each line. Thus the originator's tabulation cannot be reproduced.
- (c) Replace the letters "Z" and "J" in the decrypted version with "X" and "Y", respectively. (e.g., "Xone," "Xero," "Xamary," "Adjyust.")

9. On 20 October a working party of Subcommittee A visited the Teletype Corporation to inspect and discuss the U.S. "PCM" in the hope that some means might be devised whereby the U.S. cipher machine "PCM" plus the CSP 5000 (Automatic Off-Line Equipment) and the British cipher

~~TOP SECRET~~

~~TOP SECRET~~

machines "PENDRAGON" or "SINUS" could interwork, while still being capable of working with existing cipher machines of the nation concerned and also providing the facilities required by that nation.

10. We have further considered the matter of Teleprinter facilities and make the following recommendations:

- (a) That this Third Report of Subcommittee A be made available to the UK/US JCEC with the request that, as a matter of urgency, discussion be opened on what Teleprinter functions, upper case characters, and other facilities should be provided in new Off-Line Combined Cipher machines which permit automatic encryption and decryption in page form.
- (b) That the British, as a matter of urgency, give consideration to the U.S. proposal that Bigramming and functional signals for British machines employing the 7-rotor BOM crypto technique should be achieved by the use of the following primary characters:

<u>Primary Character</u>	<u>Function</u>	<u>To Be Linked to</u>
K	Bigram	D
J	Figure Shifts	Y
V	Letter Shifts	(Nothing)
Z	Space	X
C/R	Carriage Return	G
L/R	Line Feed	Q

- (c) That the U.S. consider the possibility of providing full Teleprinter facilities in future machines employing the 7-rotor BOM crypto technique, by utilizing the Bigram function included in the design of the British "PENDRAGON."
- (d) That since provision has been made in the British "PENDRAGON" for "Line Feed" and "Carriage Return" signals to be generated where required by suitable counting mechanisms, the British should give consideration to abandoning Bigramming and accepting the loss of two lower case characters (J and Z) and three upper case characters (upper case J, upper case Z, and upper case V) as is at present contemplated in U.S. design.

~~TOP SECRET~~

~~TOP SECRET~~

(e) That interchange of views, in particular, on recommendations
(b), (c), and (d) above, be continued.

F. R. W. Burton Miller

F. R. W. BURTON MILLER
Chairman, British Delegation

L. F. Safford

L. F. SAFFORD
Captain, U.S.N.
Chairman, U.S. Delegation

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

Third Report of Subcommittee A

24 October 1950

1. As recorded in the second report of Subcommittee A, this Subcommittee was reconvened on 23 October 1950 to consider the matter of encrypting letters plus numerals plus certain other Teleprinter characters, using the 7-rotor BCM crypto technique.

2. Subcommittee A has already recommended that the present CCM be replaced by the 7-rotor BCM crypto principle not later than 1 January 1955.

3. This replacement can be effected by both nations by modifying existing equipment and/or by introducing new equipment.

4. With the introduction of the new BCM crypto principle, the following operating facilities will be available:

- (a) Texts consisting either of 26 letters plus space, *or, but not including numerals* alternatively of 10 numerals plus one additional symbol, *but not including letters* plus space may be encrypted. On decryption "Z" will *print* decrypt as "X" as with the present CCM.
- (b) None of the additional facilities, *for example, a mixture of letters and figures* offered by a standard Teleprinter will be available.

5. The U. S. and the British are currently building new off-line cypher machines capable of employing the 7-rotor BCM principle and offering some or all of the facilities inherent in standard Teleprinters. The technique by which these facilities will be provided is different in the U.S. design from that employed in the British design, *due to differences in operating requirements as set forth in* ~~The basic reason for this is that~~ *Para. 7 and below* ~~the operating requirements as defined by each nation differ.~~

6. *General* ~~Whereas~~ both nations are ~~in general~~ agreed that the following requirements, if possible, be met:

- (a) Size and weight of the machine must show a marked reduction compared with *existing* ~~earlier~~ machines.
- (b) Encryption must be automatic to the greatest possible extent and to the lowest possible echelon.
- (c) Mechanical and cryptographic deficiencies found in the CCM and earlier machines must be eliminated. Greater reliability and simpler maintenance and adjustment must also be provided.
- (d) Essential Teleprinter facilities must be provided.

~~TOP SECRET~~

It is in the interpretation of this last requirement that the U. S. and British views are at variance.

7. The British Operational Staff require that off-line machines which are to provide automatic encryption and decryption shall be capable of:

- (a) Accepting a tape, perforated on any Teleprinter employing the International Alphabet No. 2.
- (b) Presenting automatically in page form the decrypted version identical with the original text. (Thus all the Teleprinter functions required for ~~tabulation~~ tabulation which appeared in the original text must be reproduced ~~after~~ ^{directly} decryption and be capable of operating a standard Teleprinter.)

8. ^{specified} ~~The~~ U. S. operational requirement has not been so ^{exactly} clearly defined. The term "Essential Teleprinter Facilities" has been employed and is currently interpreted by the designers as requiring that the machine must be capable of receiving a Plain Language Tape perforated on any standard Teleprinter and must produce the decrypted version in page form. To provide these facilities the U. S. designers:

- (a) ^{use} ~~ignore~~ some ^{but not all} of the upper case characters. (add alter)
- (b) Insert "Carriage Return" and "Line Feed" ~~in the decrypted version at a position determined by the receiving device.~~ ^{during decryption} ~~only~~ ^{at the end of each line} ~~position determined by the receiving device.~~ ^{cannot be reproduced} ~~is not possible~~ Thus the originator's tabulation
- (c) Replace the letters "Z" and "J" in the decrypted version with "X" and "Y", respectively. (e.g., "Xone", "Xero", "Yanuary", "Adjust".)

9. On 20 October a working party of Subcommittee A visited the Teletype Corporation to inspect and discuss the ^{cipher machine} U. S. "PCM" in the hope that some means might be devised whereby the U. S. "PCM" plus the CSP 5000 (Automatic Off-Line Equipment) and the ^{cipher machines} British "PENDRAGON" or "SINGLET" could interwork, while still being capable of working with existing ^{cipher} machines of the nation concerned and also providing the facilities required by that nation.

~~TOP SECRET~~

~~TOP SECRET~~

10. We have further considered the matter of Teleprinter facilities and make the following recommendations:

(a) That the recommendation contained in the First Report of Subcommittee A, namely "That the British accept the cryptographic principles of the BCM as a replacement for the CCM in combined communications" should stand without modification.

(b) That this Third Report of Subcommittee A be made available to the UK/US JCEC with the request that, as a matter of urgency, discussion be opened on what ^{functions, and upper case characters, and other} Teleprinter facilities should be provided in new Off-line Combined Cypher machines which permit automatic encryption and decryption in page form.

(c) That the British, as a matter of urgency, give consideration to the U. S. proposal that Bigramming and functional signals for British machines employing the 7-rotor BCM crypto technique should be achieved by the use of the following primary characters:

<u>Primary Character</u>	<u>Function</u>	<u>To Be Linked to</u>
K	Bigram	D
J	Figure Shift	Y
V	Letter Shift	(Nothing)
Z	Space	X
G/R	Carriage Return	C
L/F	Line Feed	G

(d) That the U. S. ~~as a matter of urgency~~, consider the possibility of providing full Teleprinter facilities in future machines employing the 7-rotor BCM crypto technique, by utilizing the Bigram function included in the design of the British "PENDRAGON".

(e) ~~That~~ Since provision has been made in the British "PENDRAGON" for "Line Feed" and "Carriage Return" signals to be generated where required by suitable counting mechanisms, the British should give consideration

~~TOP SECRET~~

~~TOP SECRET~~

to abandoning Elgramming and accepting the loss of two lower case characters (J and Z) and three upper case characters (upper case J, upper case Z, and upper case V) as is at present contemplated in U. S. design.

(P) That interchange of views, in particular, on recommendations ^b(a), ^c(d), and ^d(e) above, be continued ~~through existing channels.~~

T. R. W. Burton Miller

T. R. W. BURTON MILLER
Chairman, British Delegation

L. F. Safford

L. F. SAFFORD
Captain, U.S.N.
Chairman, U.S. Delegation

~~TOP SECRET~~

~~TOP SECRET~~

Friedman

BRUSA COMSEC CONFERENCE

Second Report of Subcommittee A

10 October 1950

1. As directed, Subcommittee A was reconvened and met on Monday, 9 October, and Tuesday, 10 October 1950, at which time the following recommendations to be forwarded to the Executive Committee for approval were unanimously adopted by the Subcommittee:

a. Encryption of Literal Texts

This aspect has already been covered in the first report of Subcommittee A.

b. Encryption of Numerals Plus "X" or "Slash"

On the assumption that there is a Combined requirement for the encryption on the agreed Combined cryptosystem of texts consisting of the numerals plus "X" or "Slash," we recommend that the necessary facility shall be provided as soon as it is available, where required.

c. Encryption of Letters, Plus Numerals, Plus Certain other Teleprinter Characters

It is apparent that the U.S. and the British have been called on to meet differing operational requirements. This has resulted in the design authorities of the two countries proceeding along different lines of development. A possible compromise between these conflicting developments has recently been put forward from the U. S. side and a working party consisting of:

U.S.
 Captain L. F. Safford, USN
 Commander D. W. Seiler, USN
 Commander G. W. Linn, USN

British
 Lt. Colonel C. A. Henn-Collins
 Mr. E. H. Jolley

has been appointed to investigate the proposal. On Friday, October 20th, Captain Safford will escort the British members of the working party on a visit to the Teletype Corporation where the PCM (CSP 4700) and the new Off-Line Automatic Equipment (CSP 5000) which materially affect this aspect are under development. The working party will resume discussions on Monday, 23 October, and report in due course to Subcommittee A.

T. R. W. Burton Miller
 T. R. W. BURTON MILLER
 Chairman, British Delegation

L. F. Safford
 L. F. SAFFORD
 Captain, U.S.N.
 Chairman, U.S. Delegation

~~TOP SECRET~~

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

First Report of Subcommittee A

21

(As modified by the Combined Executive Committee on 27 September 1950)

26 September 1950

1. Subcommittee A has held five meetings to date, viz., morning and afternoon of 22 September, morning of 23 September, afternoon of 25 September, and afternoon of 26 September.

2. Membership of the Subcommittee:

British Members

Mr. T. R. W. Burton Miller, Head of Mission
 Captain, the Earl Cairns, R. N.
 Mr. Kenneth Perrin
 Mr. J. M. G. Pollard
 Lt. Colonel C. A. Henn-Collins
 Mr. E. H. Jolley

U. S. Members

Captain L. F. Safford, USN, AFSA COX, Chairman

Representing JOEC:

Commander F. C. Concannon, USN
 Lt. Col. T. J. Trainor, USA (Alternate: Major J. R. Carpenter, USA)
 Major J. M. Anderson, Jr., USAF (Alternate: Maj. R. W. Larson, USAF)

Representing Service Cryptologic Agencies:

Mr. Richard Batty, ASA (Alternate: Mr. Warren Beck)
 Cdr. F. C. Concannon, USN, Op-202 (Alternate: Cdr. G. W. Linn, USN)
 Major Phillip Evans, USAF, AFSS (Alternate: Maj. G. E. Parr, USAF)

Representing AFSA:

Commander D. W. Seiler, USN, AFSA-04
 Dr. A. Sinkov, AFSA-04 (Alternate: Mr. R. H. Shaw)
 Colonel R. C. Sears, USAF, AFSA-03 (Alternate: Mr. Leo Rosen)
 Mr. Mark Rhoads, AFSA-14, (Member and Recorder)

3. The first meeting was attended by the following persons in addition to the regular members:

Admiral Earl E. Stone, USN
 Brigadier John H. Tiltman, British SLO
 Colonel S. P. Collins, AFSA-00A
 Captain H. O. Hansen, AFSA-04
 Mr. W. F. Friedman, AFSA-00T
 Commander J. R. G. Trechman, British JSM
 Lt. Col. Russell H. Horton, AFSA-12A, Recorder

4. The first meeting was devoted to an outline of the scope of the subjects to be covered by Subcommittee A, viz., the replacement of the CCM by the U. S. 7-rotor BCM and/or the U.S. PCM, certain auxiliary automatic equipment,

~~TOP SECRET~~

~~TOP SECRET~~

improvements in rotor design, and security improvements of present CCM as proposed by the U.S. JCS in 2074/2 dated 27 December 1949. The 7-rotor BCM (CSP 4800) was exhibited and demonstrated at this meeting.

5. At the second meeting the British outlined their general problem. They are willing to accept the 7-rotor BCM cryptographic principle, and discussions ensued as to how its adoption would fit in with present and long range plans. Also discussed was how and what automatic teleprinter equipment could be used with the 7-rotor BCM, and how the small version called the PCM fitted into the picture.

6. The third meeting on Saturday morning, 23 September, included exhibition and operation (where practicable) of:

- a. CSP 5100 Reader working with 7-rotor BCM (CSP 4800).
- b. CSP 1700 (modified by substituting ENG-308 translator for ENG-108 printer) working with the AN/GGA-1 Off-line Equipment.
- c. Drawing of the CSP 5000 (small Off-line Equipment).
- d. PCM (Mock-up, photographs and stepping diagram [schematic diagram not available]).
- e. PCM and BCM rotors, with examples of interchangeable notch patterns and bobbin wiring.

7. The fourth meeting was held on Monday afternoon after the British had had an opportunity to discuss the U. S. exhibits among themselves. After some discussion the following recommendations to be forwarded to the Executive Committee for approval were unanimously adopted by the Subcommittee:

- a. The British will accept the cryptographic principles of the 7-rotor BCM as a replacement for the CCM in combined communications.
- b. Except by mutual agreement, disclosure of the 7-rotor BCM principle will be limited to the U.S. and to the British Commonwealth. The British agree to notify the U. S. authorities when any issue of a combined 7-rotor BCM system is made to a nation of the British Commonwealth.
- c. The target date for full implementation of the 7-rotor BCM is set as 1 January 1955 or sooner if circumstances permit. Limited introduction, where a small number of machines would be involved, should be implemented at the earliest practicable date.

~~TOP SECRET~~

~~TOP SECRET~~

d. Rotors on both U.S. and British versions of the 7-rotor BCM to be physically and cryptographically interchangeable. This means that the British will change to the size now used in CSP 1700. All data, manufacturing, and wiring details to be furnished to the British for this purpose.

e. The British and U.S. will make independent security studies on the 7-rotor BCM, including the following items:

- (1) Possible changes in stepping order.
- (2) Notch patterns for stepping control.
- (3) Type of rotor wiring (interval, random, or composite).
- (4) Preparation of key lists.
- (5) Indicator procedure.
- (6) Restrictions on operational use of machine for security

reasons.

- (7) And similar technical matters.

Upon completion of these studies the U.S. and the U.K. will exchange technical papers through established channels. If necessary, a special meeting to reconcile divergent views may be held in London (or Washington) at some later date.

f. The British and U. S. will prepare and exchange separate papers for purpose of reaching agreements on operating instructions, maintenance instructions, crypto-security precautions, and other procedural matters.

g. Models (when available), drawings, specifications, and operating instructions (where necessary) of the following equipments will be made available to the British:

BCM (CSP 4800)

PCM (CSP 4700) and PCM type rotor

Tape Reader (AFSAM 12 or CSP 5100)

CSP 5000 Off-line automatic equipment

ENG-308 Translator for BCM (CSP 4800)

Rotor refinements for Mark I (3"), Mark II (3 1/2"), and

Mark III (2 1/2") rotors

An/GGA-1 (Instructions only)

~~TOP SECRET~~

~~TOP SECRET~~

h. Make available to the British the tools and dies for Mark I rotors (for old Typex adapters).

i. Make available to the British the tools and drawings of old Typex adapter, new design of Typex adapter rotors with tires, and parts and drawings for new Typex adapter.

3. The following recommendations were agreed upon regarding improvement of security of present CCM until supersession date 1 January 1955 as proposed by the U.S. JCS in 2074/2 dated 27 December 1949:

a. Henceforth there will be issued 20 rotors to the set for each CCM in lieu of present number of 10. This will become effective with the next issue of new rotors. Key lists will be so prepared that no rotor will ever be effective on two successive days, within the same key lists for each cryptochannel, so as to permit setting up two baskets for two successive days from a single set of 20 rotors thus obviating the need for duplicate sets of rotors. This will result in no substantial increase in the number of rotors to be fabricated under present plans.

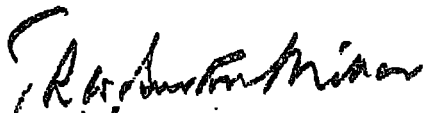
b. Removable tires will be introduced as soon as practicable after suitable rotors become available.

c. Matters such as the rate of supersession and specific times of supersession are to be left to the established agencies charged with such matters.

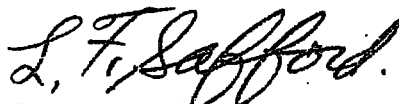
9. The U. S. will prepare criticism of the British machines, "Pendragon" and "Singlet."

10. Subcommittee A will reconvene after Subcommittee B has completed its deliberations. It is hoped that further agreement may then be reached regarding the long-range provision of facilities for automatic operations, using off-line combined cipher equipment.

11. The fifth meeting was called for committee approval of the wording of the foregoing items.



T. R. W. BURTON MILLER
Chairman, British Delegation



L. F. SAFFORD
Captain, U.S.N.
Chairman, U.S. Delegation

~~TOP SECRET~~

BRUSA COMSEC CONFERENCE

First Report of Subcommittee A

26 September 1950

1. Subcommittee A has held five meetings to date, viz., morning and afternoon of 22 September, morning of 23 September, afternoon of 25 September, and afternoon of 26 September.

2. Membership of the Subcommittee:

British Members

Mr. T. R. W. Burton Miller, Head of Mission
Captain, the Earl Cairns, R.N.
Mr. Kenneth Perrin
Mr. J. M. G. Pollard
Lt. Colonel C. A. Hemm-Collins
Mr. E. H. Jolley

U. S. Members

Captain L. F. Safford, USN, AFSA-OOX, Chairman

Representing JCEC:

Commander F. C. Concannon, USN
Lt. Col. T. J. Trainor, USA (Alternate: Major J.R. Carpenter, USA)
Major J. M. Anderson, Jr., USAF (Alternate: Maj. R.W. Larson, USAF)

Representing Service Cryptologic Agencies:

Mr. Richard Battey, ASA (Alternate: Mr. Warren Beck)
Cdr. F. C. Concannon, USN, Op-202 (Alternate: Cdr. G. W. Linn, USN)
Major Phillip Evans, USAF, AFSS (Alternate: Maj. G.E. Parr, USAF)

Representing AFSA:

Commander D. W. Seiler, USN, AFSA-O4
Dr. A. Sinkov, AFSA-O4 (Alternate: Mr. R. H. Shaw)
Colonel R. C. Sears, USAF, AFSA-O3 (Alternate: Mr. Leo Rosen)
Mr. Mark Rhoads, AFSA-14 (Member and Recorder)

3. The first meeting was attended by the following persons in addition to the regular members:

Admiral Earl E. Stone, USN
Brigadier John H. Tiltman, British SLO
Colonel S. P. Collins, AFSA-OQA
Captain H. O. Hansen, AFSA-O4
Mr. W. F. Friedman, AFSA-OOT
Commander J.R.G. Trechman, British JSM
Lt. Col. Russell H. Horton, AFSA-12A Recorder

4. The first meeting was devoted to an outline of the scope of the subjects to be covered by Subcommittee A, viz., the replacement of the CCM by the U.S. 7-rotor BCM and/or the U.S. PCM, certain auxiliary automatic equipment,

improvements in rotor design, and security improvements of present CCM as proposed by the U.S. JCS in 2074/2 dated 27 December 1949. The 7-rotor BCM (GSP 4800) was exhibited and demonstrated at this meeting.

5. At the second meeting the British outlined their general problem. They are willing to accept the 7-rotor BCM cryptographic principle, and discussions ensued as to how its adoption would fit in with present and long range plans. Also discussed was how and what automatic teleprinter equipment could be used with the 7-rotor BCM, and how the small version called the PCM fitted into the picture.

6. The third meeting on Saturday morning, 23 September, included exhibition and operation (where practicable) of:

- a. GSP 5100 Reader working with 7-rotor BCM (GSP 4800).
- b. GSP 1700 (modified by substituting ENG-308 translator for ENG-108 printer) working with the AN/GGA-1 Off-line Equipment.
- c. Drawing of the GSP 5000 (small Off-line Equipment).
- d. PCM (Mock-up, photographs and stepping diagram ^{AFSAH-17} schematic diagram not available).
- e. PCM and BCM rotors, with examples of interchangeable notch patterns and bobbin wiring.

7. The fourth meeting was held on Monday afternoon after the British had had an opportunity to discuss the U. S. exhibits among themselves. After some discussion the following ^{recommendations} ~~agreements~~ to be forwarded to the Executive Committee for approval were unanimously adopted by the Subcommittee:

- a. The British will accept the cryptographic principles of the 7-rotor BCM as a replacement for the CCM in combined communications.
- b. Except by ^{mutual} initial agreement, ^{disclosure of the 7-rotor BCM principle} ~~distribution of this machine~~ will be limited to the U.S. and British Commonwealth. The British agree ^{of a Combined 7-rotor BCM System} to notify the U.S. authorities when any issue is made to a ^{Member of the} ~~Member of the~~ British Commonwealth. ^{to the} ^{nation}
- c. The target date for full implementation of the 7-rotor BCM is set as 1 January 1955 or sooner if circumstances permit. Limited introduction, where a small number of machines would be involved, should be implemented at the earliest practicable date.

d. Rotors on both U.S. and British versions of the 7-rotor ECM to be physically and cryptographically interchangeable. This means that the British will change to the size now used in CSP 1700. All data, manufacturing, and wiring details to be furnished to the British for this purpose.

e. The British and U.S. will make independent security studies on the 7-rotor ECM, including the following items:

- (1) Possible changes in stepping order.
- (2) Notch patterns for stepping control.
- (3) Type of rotor wiring (interval, random, or composite).
- (4) Preparation of key lists.
- (5) Indicator procedure.
- (6) Restrictions on operational use of machine for security reasons.

(7) And similar ^{technical} matters.

Upon completion of these studies the U.S. and U.K. will exchange ^{the} papers ^{technical} through ^{protected channels} and ~~attempts to reconcile divergent views~~ ^{to reconcile divergent views} agreement will be sought through the facilities of U.S./U.K. JCRC. If necessary, a special meeting may be held in London (or Washington) at some later date, ~~to reach a firm agreement on these points.~~ ^{Final agreement will be}

f. The British and U.S. will prepare and exchange separate papers for purpose of reaching ~~an~~ agreement on operating instructions, maintenance instructions, crypto-security precautions, and other procedural matters.

g. Models (when available), drawings, specifications, and operating instructions (where necessary) of the following equipments will ^{made available} be ~~given~~ to the British:

- BCM (CSP 4800)
- PCM (CSP 4700) and PCM type rotor
- Tape Reader (AFSAM 12 or CSP 5100)
- CSP 5000 Off-line automatic equipment
- ENG-308 Translator for BCM (CSP 4800)
- Rotor refinements for Mark I (3"), Mark II (3 1/2"), and Mark III (2 1/2") rotors

AN/GGA-1 (Instructions only)

~~TOP SECRET~~

- h. Make ^{available} ~~indefinite loan~~ ^{to} British ^{of} tools and dies for Mark I rotors ^(for TypeX adapter) ~~for TypeX adapter~~ ^{available} ~~to~~ British ^{of} tools and dies for
- i. Make ^{available} ~~indefinite loan~~ ^{to} British ^{of} tools and drawings of old TypeX adapter, new design of TypeX adapter rotors with tires, and parts and drawings for new TypeX adapter.
8. The following ^{recommendations were agreed upon} ~~agreements were made~~ regarding improvement of security of present CCM until supersession date 1 January 1955 as proposed by the U.S. JCS in 2074/2 dated 27 December 1949:
- a. Henceforth there will be issued 20 rotors to the set for each CCM in lieu of present number of 10. This will become effective with the next issue of new rotors. Key lists will be so prepared that no rotor will ever be effective on two successive days, within the same key lists for each cryptochannel, so as to permit setting up two baskets for two successive days from a single set of 20 rotors thus obviating the need for duplicate sets of rotors. This will result in no substantial increase in the number of rotors to be fabricated under present plans.
- b. Removable tires will be introduced as soon as practicable after suitable rotors become available.
- c. Matters such as the rate of supersession and specific times of supersession are to be left to ^{established agencies} ~~the regular U.S./U.K. combined JCEC~~ charged with such matters.
9. The U. S. will prepare criticism of the British machines, "Pendragon" and "Singlet."
10. Subcommittee A will reconvene after Subcommittee B has completed its deliberations. It is hoped that further agreement may then be reached regarding the long-range provision of facilities for automatic operations, using off-line combined cipher equipment.
11. The fifth meeting was called for committee approval of the wording of the foregoing items.



T. R. W. BURTON MILLER
Chairman, British Delegation



L. F. SAFFORD
Captain, U.S.N.
Chairman, U.S. Delegation

~~TOP SECRET~~