FINAL

SUBJECT NUMBER

AFSAC: 63/65 Item 2 of the Agenda for the Thirty-eighth Meeting of AFSAC, held on 20 June 1952.

Subject: U.K./U.S. Communication Security Conference, 1952. (AFSAC 63/63)

The CHAIRMAN introduced the second item by stating that the paper under consideration (AFSAC 63/63) was a general report of the UK/US Communication Security Conference, 1952, exclusive of the technical papers of the Conference. He then invited attention to paragraphs 9a through 9d which set forth the crypto systems which were to be offered for NATO adoption. He stated that the subparagraphs in question contained, in addition to security implications, [redacted] implications that should be carefully weighed by AFSAC.

The CHAIRMAN continued by saying that the first aspect of the problem was that the [redacted] that the British delegation to the subject Conference was acting under these instructions in making such recommendations in the Conference report. In view of this, he concluded, it appeared advisable that the question of whether [redacted] was foremost to the interests of the U.S. should be resolved by the appropriate US authorities. Toward this end, he suggested that the question be forwarded to USCIB for forwarding to the National Security Council for resolution.

The other aspect of the problem, the CHAIRMAN continued, concerned the similarity between Circuit Mercury and CSP 2900. He stated that Circuit Mercury was analogous to and superior to the CSP 2900, and that, although CSP 2900 had been held as a strictly national system, approval of the Conference report would constitute a recommendation that a system superior to the CSP 2900 be released to all the NATO nations even though, under present U.S. policy, CSP 2900 could not be released, even to the British.

The CHAIRMAN concluded by saying that it had been known for some time that the British were well aware of the existence and capabilities of the CSP 2900. He added that it therefore would be extremely unrealistic to continue to withhold CSP 2900 from them for the reason that we did not want to divulge the ECM principle. He also said that he had requested of Mr. Burton Miller that Circuit Mercury not be included in the list of systems proposed for NATO use, but that the British had been insistent in including it. His agreement to the Conference report, he stated, had been made nevertheless, knowing that the report would not become final until it had been approved by the JCS.

COPY #_____

The CHAIRMAN then requested the views of the members.

[redacted]

The CHAIRMAN replied that he had singled out Mercury because it was tied in with the CSP 2900 problem. He pointed out that the U.S. had already released the AFSAM 7 and AFSAM 47 for NATO use, and added that the problem involved the overall implications [redacted] rather than MERCURY alone. He also expressed the personal opinion that Communication Security should precede [redacted] considerations.

GENERAL DUFF referred to the U.S. policy that the best Crypto principal be reserved exclusively for U.S. use and inquired what such a system would be.

After a brief discussion of the principles of the CSP 2900 and Circuit Mercury by Mr. Friedman, the CHAIRMAN commented that CSP 2900 was not the best system. He added that the Navy had the CSP 2300, a modification of the CSP 2900, which was superior to the 2900.

CAPTAIN HOWETH stated that the decision to reserve the CSP 2900 had been made after the 1951 COMSEC Conference when there were insufficient quantities of the CSP 2300 to consider it as a system.

A brief discussion of the various systems followed and Mr. FRIEDMAN pointed out some facts which further established the point that the British are fully informed on the principles of the ECM and, in addition, have some knowledge of the CSP 2900.

CAPTAIN HOWETH expressed the opinion that the original reason for withholding one system for exclusive U.S. use was the possibility that at some time the British Commonwealth might collapse.

ADMIRAL WENGER confirmed that such a possibility had been considered and added that the consideration of flexibility alluded to by the Chairman was also among the other reasons for withholding an exclusive U.S. system.

CAPTAIN HOWETH inquired if MERCURY could be made compatible with CSP 2900.

MR. FRIEDMAN commented that it probably could not.

CAPTAIN HOWETH inquired if there was still security to be gained by maintaining the CSP 2900 exclusively as a U.S. system.

The CHAIRMAN replied that the experts assured him that the security of the machine was dependent upon the security of the key lists and rotors.

CAPTAIN HOWETH stated that he had never been able to accept that opinion.

The CHAIRMAN also stated that, against known exhaustion attacks, the CSP 2900 was secure. He added that he was not in favor of giving the CSP 2900 to NATO although it could be offered for high level Combined use. He also stated that 200 machines would be required for high level Combined communications and 1000 for general Combined communications and added that since we did not have sufficient quantities to solve the NATO problem, there was nothing to gain in discussing that problem at the present time.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

The CHAIRMAN agreed that it was not possible.

CAPTAIN HOWETH expressed the opinion that [redacted] would not dry up completely but that it would be materially reduced. He added that

[redacted]

The CHAIRMAN commented that the NATO requirements for diplomatic communications would be insignificant. He then stressed the implications of the problem on [redacted] and expressed the opinion that the other intelligence people who were not represented here should have an opportunity to express an opinion in the matter. The other aspect of the problem, he stated, was strictly the concern of the Services and the Joint Chiefs of Staff.

The CHAIRMAN restated the issue by saying the release of a highly secure system to NATO would enable the NATO countries to improve the security of all of their communications. In addition, because of laxness of security in NATO countries, potential opponents and non-NATO nations would soon obtain knowledge of these systems and thereby increase the security of their communications. The end result, he stated, would be to materially reduce the quantity [redacted]

MR. FRIEDMAN expressed another reason for advising USCIB of the problem. He stated that it might be possible for the U.S., through an extremely expensive [redacted] development program, to devise rapid analytical machinery that would enable the U.S. to come out on top of the game, purely by virtue of physical resources. He added that the members of USCIB should be thinking in terms of such an eventuality if [redacted] were to be maintained.

GENERAL SAMFORD made a motion that the question of whether COMSEC [redacted] was foremost to the interests of the U.S. be forwarded, via USCIB, to the National Security Council for resolution.

This was agreed.

ADMIRAL AMMON proposed that the second aspect of the problem concerning the report of the UK/US COMSEC Conference and the release of circuit Mercury to NATO be referred to an ad hoc committee for study and recommendation.

CAPTAIN HOWETH added that the ad hoc group should also consider the implications of the possible release of CSP 2900 to the British for Combined use.

This was agreed.

It was also agreed that the Chairman, AFSAC, would apprise the Joint Chiefs of Staff that the problem of whether COMSEC [redacted] was foremost to the interests of the U.S. had been forwarded to the NSC for resolution.

The CHAIRMAN called the first meeting of the ad hoc committee for 1330 on Tuesday, 24 June 1952, in Room 19-125 Naval Security Station, and requested that the composition of the ad hoc committee be limited to one member from each Service and one from AFSA.

DECISION: (20 June 1952) AFSAC agreed:

(1) to forward to the N.S.C. for adjudication, via USCIB, the question of whether Communication Security [redacted] is foremost to the interests of the U.S.

(2) that the Chairman, AFSAC, would apprise the Joint Chiefs of Staff of the foregoing decision.

(3) that an ad hoc committee be formed to study the implications of para 9d of the report of the UK/US COMSEC Conference (AFSAC 63/63) which recommended the release of circuit Mercury to NATO, and to study the question of the release of the CSP 2900 to the British, for purely Combined use, as an interim solution to the replacement of the CCM.
It was also agreed that the first meeting of the ad hoc committee would be held at 1330 on Tuesday, 24 June 1952, in Room 19-125, NavSecSta, and that the composition would be limited to one member from each Service and one member from AFSA.

This item to be continued on the agenda.