

~~TOP SECRET~~

57

AFSAC: 63/74

24 February 1954

~~TOP SECRET~~MEMORANDUM FOR THE MEMBERS OF AFSAC:

Subject: Report of the U.K./U.S. Communication Security Conference, 1953.

1. The inclosure is forwarded for your information and retention.
2. Downgrade to UNCLASSIFIED when the inclosure is removed.

William R. Statler
WILLIAM R. STATLER
Secretary, AFSAC

Inclosure - 1

Note by the Secretaries to the Holders of J.C.S. 2074/29,
dated 10 February 1954, Copy No. 51.

AFSAC: 63/74

~~TOP SECRET~~

~~CONFIDENTIAL~~COPY-NO. 5710 February 1954

(LIMITED DISTRIBUTION)

NOTE BY THE SECRETARIES

to the

HOLDERS OF J.C.S. 2074/29

(Report of the U.K./U.S. Communication Security Conference, 1953)

Pursuant to an agreement by the Joint Chiefs of Staff on 9 February 1954, J.C.S. 2074/29 and J.C.S. 2074/30 were referred by SM-128-54, dated 11 February 1954, to the Armed Forces Security Agency Council for comment and recommendation.

EDWIN H. J. CARNES,

RICHARD H. PHILLIPS,

Joint Secretariat.

DISTRIBUTION

Adm. Radford (C/JCS)

Gen. Ridgway (CSA)

Adm. Carney (CNO)

Gen. Twining (CSAF)

Gen. Lemnitzer (DC/S,P)

Gen. Eddleman (Asst. C/S, G-3)

Adm. Gardner (DCNO-Op)

Adm. Burke (ACNO-Op30)

Gen. Partridge (DC/S-Op, Air)

Gen. Thatcher (Dir. Plans, Air)

Gen. Everest (D/JS)

Gen. Porter (DDI)

Secy, JCS

Secy, JSSC

Secy, JCEC

~~CONFIDENTIAL~~

Note to Holders of JCS 2074/29

MEMO ROUTING SLIP		NEVER USE FOR APPROVALS, CONCURRENCES, OR SIMILAR ACTIONS	
1	NAME OR TITLE	INITIALS	CIRCULATE
	ORGANIZATION AND LOCATION	DATE	COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE
REMARKS			
<p>See D5C18 Papers of 23/- Series</p>			
FROM NAME OR TITLE		DATE	
ORGANIZATION AND LOCATION		TELEPHONE	

~~TOP SECRET~~

Ser 00016P20

17 February 1954

ARMED FORCES SECURITY AGENCY COUNCIL

REPORTTO THE U.S. JOINT CHIEFS OF STAFFTHE PROBLEM

1. To consider the report of the fourth UK/US communication security conference held in London during October and November 1953.

FACTS BEARING ON THE PROBLEM

2. In 1950 it was agreed to continue for the next four years the series of UK/US communication security conferences begun that year. The report under consideration covers the fourth such conference, held in London during October and November, 1953. A copy of the report is contained in JCS 2074/29.

3. The conference discussed and made recommendations concerning the following matters:

- a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem;
- b. On-line teletypewriter cypher machines;
- c. Spurious emissions which endanger communications security;
- d. Speech security equipments;
- e. Facsimile security equipments (CIFAX);
- f. Transmission security;
- g. Non-communications transmissions;
- h. Weather cryptosystems;
- i. Communications Security Development Programme;
- j. Exchange of equipments and components;
- k. Effects of advances in electronics;
- l. Co-ordination of Cryptographic and Communications Equipment Development;
- m. Operating and Maintenance;
- n. Standards of Security Requirements;
- o. Future Liaison.

~~TOP SECRET~~

~~TOP SECRET~~

4. Under date of 9 February 1954, the British Joint Services Mission notified the Secretary, U.S. Joint Chiefs of Staff of the U.K. Chiefs of Staff approval of the subject report.

DISCUSSION

5. Paragraph 5.a. of the report refers to "the U.S. cryptoprinciple embodied in the AFSAM 7". Inasmuch as AFSAM 47B embodies the same principle as this AFSAM 7, the conference recommendation should be changed to reflect this fact. At the same time it should be noted that while the AFSAM 7 is in production, the AFSAM 47B will not be in full production until later this year, the report should be clarified on this point.

6. In paragraph 5.e. of the report it is stated that "the CAN-UK-US JCECs have already agreed that multi-channel sub-carrier frequency modulation is the best method of transmission for CIFAX-----". While the conferees had been informed prior to the conference that such an agreement had been reached, this information was in error, and no combined agreement on the subject of a transmission system for enciphered facsimile exists. Therefore, the conference recommendation on this subject should be deleted.

7. The conference makes certain recommendations in paragraph 5.f. of the report concerning transmission security. In order to isolate this problem from that of censorship of civil communications, the report should be modified to show that military communications only are involved. The phrase "insecure means" should also be more clearly defined.

8. In paragraph 5.g. of the report recommendations are made concerning security of Mark X IFF. Since "SIF with IFF Mark X" is neither cryptographic nor communication security equipment it was not an appropriate subject for discussion at the conference. The entire conference recommendation on this subject should therefore be disapproved and deleted.

CONCLUSIONS

9. It is concluded:

a. That the conference report should be modified to reflect the fact that the same cryptoprinciple is contained both in AFSAM 7 and AFSAM 47B, but that the latter will not be in production until a later date.

~~TOP SECRET~~

~~TOP SECRET~~

b. That the conference recommendation concerning a sub-carrier frequency modulation transmission system for combined use with enciphered facsimile (CIFAX) should be deleted.

c. That the conference recommendation concerning transmission security should be modified to indicate clearly that military communications only are involved, and also more clearly to define insecure transmission means.

d. That the conference recommendation concerning use of SIF with IPF Mark X should be disapproved and deleted from the report.

RECOMMENDATIONS

10. It is recommended:

a. That the foregoing conclusions be approved.

b. That the conference report be approved except for the matters covered in the foregoing conclusions.

c. That a memorandum substantially as in enclosure "A" hereto be forwarded to the representative of the British Chiefs of Staff.

d. That a memorandum substantially as in enclosure "B" hereto be forwarded to the Director, National Security Agency.

~~TOP SECRET~~

~~TOP SECRET~~ENCLOSURE "A"MEMORANDUM FOR THE REPRESENTATIVES OF
THE BRITISH CHIEFS OF STAFF

1. The United States Joint Chiefs of Staff approve, with the minor exceptions noted below, the report of the UK/US Communications Security Conference 1953.

2. It is recommended that the report be changed as follows:

a. Paragraph 5.a., in first sentence of the text the term "AFSAM 7" should read "AFSAM 7 and AFSAM 47B", and the words "the former" should be inserted before the phrase "now in production in the U.S.A." In the last sentence the term "AFSAM 7" should read "AFSAM 7 and AFSAM 47B". These changes are recommended inasmuch as the same cryptoprinciple is embodied in both AFSAM 7 and AFSAM 47B.

b. Paragraph 5.e., delete all after the first sentence of the text inasmuch as the CAN-UK-US JCECs have not yet reached agreement on a transmission system for enciphered facsimile. It is regretted that the conferees were provided incorrect information on this point.

c. Paragraph 5.f., first sentence, insert the word "military" between the words "unclassified" and "messages", in order clearly to isolate the problem from the problem of civil communications, which is essentially a matter of censorship. Also, in the same sentence, insert parenthetically the phrase "(radio and sensitive wire circuits)" between the words "insecure" and "means". This change will more clearly express the intent of the wording.

3. The U.S. view is that the LFF Mark X system with Selective Identification Feature is neither cryptographic nor communications security equipment and that it was not an appropriate subject for discussion at this conference. The U.S. Joint Chiefs of Staff therefore disapprove the recommendations of paragraph 5.g. and recommend the deletion of all but the first three sentences.

4. The United States Joint Chiefs of Staff wish to express their satisfaction with the result of the 1953 conference, especially the

~~TOP SECRET~~

Enclosure "A"

~~TOP SECRET~~

agreements reached on the problem of replacing the existing combined and NATO High Grade off-line cryptosystem. Every possible action is being taken to implement the replacement of this general cryptosystem.

5. For the next conference, to be held in Washington, the United States Joint Chiefs of Staff suggest that the opening date be as agreed between the Director, National Security Agency, and the Chairman, Cypher Policy Board.

~~TOP SECRET~~

Enclosure "A"

~~TOP SECRET~~ENCLOSURE "B"MEMORANDUM FOR THE DIRECTOR,
NATIONAL SECURITY AGENCY

1. The U.S. Joint Chiefs of Staff have considered the report of the UK/US Communications Security Conference 1953. A copy of a memorandum to the Representatives of the British Chiefs of Staff on this subject is attached hereto as enclosure "A".

~~TOP SECRET~~

Enclosure "B"

~~TOP SECRET~~

Ser 00016P20

17 February 1954

ARMED FORCES SECURITY AGENCY COUNCIL

REPORTTO THE U.S. JOINT CHIEFS OF STAFFTHE PROBLEM

1. To consider the report of the fourth UK/US communication security conference held in London during October and November 1953.

FACTS BEARING ON THE PROBLEM

2. In 1950 it was agreed to continue for the next four years the series of UK/US communication security conferences begun that year. The report under consideration covers the fourth such conference, held in London during October and November, 1953. A copy of the report is contained in JCS 2074/29.

3. The conference discussed and made recommendations concerning the following matters:

- a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem;
- b. On-line teletypewriter cypher machines;
- c. Spurious emissions which endanger communications security;
- d. Speech security equipments;
- e. Facsimile security equipments (CIFAX);
- f. Transmission security;
- g. Non-communications transmissions;
- h. Weather cryptosystems;
- i. Communications Security Development Programme;
- j. Exchange of equipments and components;
- k. Effects of advances in electronics;
- l. Co-ordination of Cryptographic and Communications Equipment Development;
- m. Operating and Maintenance;
- n. Standards of Security Requirements;
- o. Future Liaison.

~~TOP SECRET~~

~~TOP SECRET~~

4. Under date of 9 February 1954, the British Joint Services Mission notified the Secretary, U.S. Joint Chiefs of Staff of the U.K. Chiefs of Staff approval of the subject report.

DISCUSSION

5. Paragraph 5.a. of the report refers to "the U.S. cryptoprinciple embodied in the AFSAM 7". Inasmuch as AFSAM 47B embodies the same principle as this AFSAM 7, the conference recommendation should be changed to reflect this fact. At the same time it should be noted that while the AFSAM 7 is in production, the AFSAM 47B will not be in full production until later this year, the report should be clarified on this point.

6. In paragraph 5.e. of the report it is stated that "the CAN-UK-US JCECs have already agreed that multi-channel sub-carrier frequency modulation is the best method of transmission for CIFAX-----". While the conferees had been informed prior to the conference that such an agreement had been reached, this information was in error, and no combined agreement on the subject of a transmission system for enciphered facsimile exists. Therefore, the conference recommendation on this subject should be deleted.

7. The conference makes certain recommendations in paragraph 5.f. of the report concerning transmission security. In order to isolate this problem from that of censorship of civil communications, the report should be modified to show that military communications only are involved. The phrase "insecure means" should also be more clearly defined.

8. In paragraph 5.g. of the report recommendations are made concerning security of Mark X IFF. Since "SIF with IFF Mark X" is neither cryptographic nor communication security equipment it was not an appropriate subject for discussion at the conference. The entire conference recommendation on this subject should therefore be disapproved and deleted.

CONCLUSIONS

9. It is concluded:

a. That the conference report should be modified to reflect the fact that the same cryptoprinciple is contained both in AFSAM 7 and AFSAM 47B, but that the latter will not be in production until a later date.

~~TOP SECRET~~

~~TOP SECRET~~

b. That the conference recommendation concerning a sub-carrier frequency modulation transmission system for combined use with enciphered facsimile (CIFAX) should be deleted.

c. That the conference recommendation concerning transmission security should be modified to indicate clearly that military communications only are involved, and also more clearly to define insecure transmission means.

d. That the conference recommendation concerning use of SIF with IFF Mark X should be disapproved and deleted from the report.

RECOMMENDATIONS

10. It is recommended:

a. That the foregoing conclusions be approved,

b. That the conference report be approved except for the matters covered in the foregoing conclusions.

c. That a memorandum substantially as in enclosure "A" hereto be forwarded to the representative of the British Chiefs of Staff.

d. That a memorandum substantially as in enclosure "B" hereto be forwarded to the Director, National Security Agency.

~~TOP SECRET~~

~~TOP SECRET~~ENCLOSURE "A"MEMORANDUM FOR THE REPRESENTATIVES OF
THE BRITISH CHIEFS OF STAFF

1. The United States Joint Chiefs of Staff approve, with the minor exceptions noted below, the report of the UK/US Communications Security Conference 1953.

2. It is recommended that the report be changed as follows:

a. Paragraph 5.a., in first sentence of the text the term "AFSAM 7" should read "AFSAM 7 and AFSAM 47B", and the words "the former" should be inserted before the phrase "now in production in the U.S.A." In the last sentence the term "AFSAM 7" should read "AFSAM 7 and AFSAM 47B". These changes are recommended inasmuch as the same cryptoprinciple is embodied in both AFSAM 7 and AFSAM 47B.

b. Paragraph 5.e., delete all after the first sentence of the text inasmuch as the CAN-UK-US JCECs have not yet reached agreement on a transmission system for enciphered facsimile. It is regretted that the conferees were provided incorrect information on this point.

c. Paragraph 5.f., first sentence, insert the word "military" between the words "unclassified" and "messages", in order clearly to isolate the problem from the problem of civil communications, which is essentially a matter of censorship. Also, in the same sentence, insert parenthetically the phrase "(radio and sensitive wire circuits)" between the words "insecure" and "means". This change will more clearly express the intent of the wording.

3. The U.S. view is that the IFF Mark X system with Selective Identification Feature is neither cryptographic nor communications security equipment and that it was not an appropriate subject for discussion at this conference. The U.S. Joint Chiefs of Staff therefore disapprove the recommendations of paragraph 5.g. and recommend the deletion of all but the first three sentences.

4. The United States Joint Chiefs of Staff wish to express their satisfaction with the result of the 1953 conference, especially the

~~TOP SECRET~~

Enclosure "A"

~~TOP SECRET~~

agreements reached on the problem of replacing the existing combined and NATO High Grade off-line cryptosystem. Every possible action is being taken to implement the replacement of this general cryptosystem.

5. For the next conference, to be held in Washington, the United States Joint Chiefs of Staff suggest that the opening date be as agreed between the Director, National Security Agency, and the Chairman, Cypher Policy Board.

~~TOP SECRET~~

Enclosure "A"

~~TOP SECRET~~ENCLOSURE "B"MEMORANDUM FOR THE DIRECTOR,
NATIONAL SECURITY AGENCY

1. The U.S. Joint Chiefs of Staff have considered the report of the UK/US Communications Security Conference 1953. A copy of a memorandum to the Representatives of the British Chiefs of Staff on this subject is attached hereto as enclosure "A".

~~TOP SECRET~~

Enclosure "B"