57

AFSAC: 63/73

15 February 1954

~~TOP SECRET~~

MEMORANDUM FOR THE MEMBERS OF AFSAC:

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

Reference: JCS Policy Memo 39 dated 1 October 1952.

1. The inclosures are forwarded for information.

2. Attention is invited to the directive contained in the reference which sets forth the policy for the safeguarding of J.C.S. papers containing highly secret information.

3. Downgrade to UNCLASSIFIED when inclosures are removed.

William R. Statler
WILLIAM R. STATLER
Secretary, AFSAC

Inclosures - 3
1. J.C.S. 2074/29, dated 19 January 1954, Copy No. 57.
2. J.C.S. 2074/30, dated 12 February 1954, Copy No. 40.
3. J.C.S. 2074/31, dated 12 February 1954, Copy No. 40.

AFSAC: 63/73

~~TOP SECRET~~

COPY NO. 57

J.C.S. 2074/29

(LIMITED DISTRIBUTION)

19 January 1954

Pages 165 - 173, incl.

MEMORANDUM BY THE DIRECTOR, NATIONAL SECURITY AGENCY

for the

JOINT CHIEFS OF STAFF

on

REPORT OF THE U.K./U.S. COMMUNICATION SECURITY CONFERENCE, 1953

Serial 000145

11 January 1954

1. The fourth U.K./U.S. Communication Security Conference was held in London in November, 1953.

2. A report of the conference is attached as Enclosure "B" and the items discussed are indicated in paragraph 2 thereof. A similar report is being forwarded to the British Chiefs of Staff by the Chairman of the U.K. Delegation. I have forwarded a copy of the report to the Director, Communications-Electronics, for his information.

3. I recommend that the Joint Chiefs of Staff:

a. Approve the report contained in Enclosure "B".

b. Forward the memorandum in Enclosure "A" to the Representatives of the British Chiefs of Staff.

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

Every possible action is being taken to implement the replacement

~~S E C R E T~~

ENCLOSURE "A"

D R A F T

MEMORANDUM FOR THE REPRESENTATIVES OF
THE BRITISH CHIEFS OF STAFF

1. The United States Joint Chiefs of Staff have reviewed and approved the report to the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff on the "UK/US Communication Security Conference, 1953."

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

3. 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, NSA, and the Chairman, Cypher Policy Board.

~~TOP SECRET~~

ENCLOSURE "B"

LCS(53)/P/R

London
10 November 1953

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

REPORT

TO THE U.K. CHIEFS OF STAFF AND THE U.S. JOINT CHIEFS OF STAFF

1. In accordance with the agreement reached by the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff following the 1952 UK/US Communications Security Conference, the 1953 UK/US Communications Security Conference has been held in London. It was preceded by two weeks of informal discussions between U.K. and U.S. Engineering and Security experts.

2. During the Conference the following subjects were discussed:

a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem.

b. Other off-line cypher machines.

c. On-line teletypewriter cypher machines.

d. Speech security equipments.

e. Facsimile security equipments.

f. Non-machine off-line cryptosystems including special purpose crypto-devices and systems.

g. Transmission security, as distinct from cryptographic security.

h. The security of non-communications transmissions, including navigational aids, IFF and data transmission.

i. Crypto-material production equipments.

3. The Conference included a full and frank exchange of views on all the items listed above, demonstrations of such equipments

as could be made available and a number of visits to establishments engaged in research and development of communications security equipment.

4. During the course of the Conference, there were, as in 1952, independent discussions regarding the production of cryptomaterial required for Combined and NATO communications. The allotment of tasks between the U.K. and the U.S. was agreed and there was a valuable exchange of production techniques and procedures. There were also useful discussions, outside the Conference, of communications procedures having security aspects and progress was made towards uniformity of practice and improved security.

5. The enclosed Reports* of the various Committees which discussed the items listed in paragraph 2 above were approved by the Conference and have been submitted to the U.K. Cypher Policy Board and the U.S. National Security Agency. The highlights and major recommendations of the Conference were as follows:-

a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem

The U.K. have accepted the U.S. cryptoprinciple embodied in the AFSAM 7, now in production in the U.S.A. The new U.K. off-line machine, at present in the development stage, will embody this principle but as the U.K. machine is not expected to be in position before 1960, the U.S. will make available some 3,500 AFSAM 7 machines to the U.K. until the U.K. machine is available, and some 3,000 machines to other NATO countries, probably in time to introduce this system for Combined and NATO communications by 1st July, 1956. The U.K. and U.S. security experts have agreed that the security provided by the existing LUCIFER system (CCM) is acceptable in

*Not received at J.C.S. Secretariat

the meantime. The Conference recommends that ultimately the cryptoprinciple embodied in the AFSAM 7 should be adopted for Combined and NATO third level use.

b. On-line teletypewriter cypher machines

Operational demands for equipment of this kind are greatly in excess of its availability. The U.K. and U.S. have a very limited number of on-line equipments in existence and others are in course of development. Long-term plans will aim at the maximum degree of standardisation, thereby reducing the lack of flexibility of communications and difficulties of maintenance caused by the present situation.

c. Spurious emissions which endanger communications security

The Conference agrees that radiation, conduction and induction from communication and crypto devices are potentially grave sources of insecurity. This subject is receiving detailed examination by both countries.

d. Speech security equipments

No speech security equipments suitable for Combined and NATO use are available at present. The U.K. and U.S. have a number of projects under development for strategic and tactical uses but as yet these have not been subjected to field trials.

e. Facsimile security equipments (CIFAX)

The U.K. and the U.S. have specific projects for black/white CIFAX under test but it is as yet too early to consider one to meet Combined requirements.

As the CAN-UK-US JCECs have already agreed that multi-channel sub-carrier frequency modulation is the best method of transmission for CIFAX for other than short distance ground-wave HF radio links, the Conference recommends that the Communications Equipment Panel of the JCECs be invited to agree a technical specification for a multi-channel SCFM transmission system for Combined use with CIFAX.

f. Transmission security

The Conference was greatly concerned that in peace time unclassified messages are transmitted in plain language by insecure means. Such messages not only lead to the revelation of intelligence but they tend to nullify the good that can be achieved by otherwise sound security practices. This is true for two reasons: because compilations of individual unclassified items often provide intelligence of Secret or even Top Secret classification, and because plain language messages, related externally to cypher messages, can jeopardise the security of the latter and of the address procedures employed with them.

Other aspects of transmission insecurity were also examined, e.g., call signs, unchanging frequencies, external characteristics of encrypted messages.

The Conference was aware of the serious operational difficulties involved in finding a solution to these problems and recommends that small Working Groups of security advisers and users should be set up by the U.K. and the U.S. to study these problems and propose their solution. The results should be exchanged between the U.K. and the U.S. and, on the basis of these, Combined plans should be made.

g. Non-communications transmissions

Neither the U.K. nor the U.S. cryptographic agencies were at this stage able to put forward any practical solution to the problem of providing security for such transmissions. It was considered that insufficient effort was as yet available for detailed study, even on a theoretical basis. If this study is to be undertaken, additional personnel or an alteration in priorities would be necessary.

On the subject of the use of SIF with IFF Mark X, the Conference recommends that the attention of the CAN-UK-US JCECs

should be directed to the fact that the security agencies of both countries agree:

(1) that the present proposal for using SIF with IFF Mark X, with code-changing on Mode I is insecure as an identification system;

(2) furthermore, that the personal and functional identities of Modes II and III could be a valuable source of intelligence to an enemy;

(3) that the CAN-UK-US JCECs be invited to restate the security requirements for a system to operate in conjunction with IFF Mark X. This specification should contain information about the degree of confidence in the identification required, and the amount of risk which would be acceptable.

(4) that when the security requirements have been received from the CAN-UK-US JCECs the cryptographic agencies of the U.S. and the U.K. should make joint technical proposals for a new and secure IFF system.

h. Weather cryptosystems

The Conference agrees that the CCM should be adopted as the off-line machine system requested in the NATO Meteorological Plan and recommends that urgent action should be taken to secure acceptance through the CECS of the Standing Group with a view to placing the material necessary to implement the plan in position by the 1st May, 1954. Very early provision should be made to equip a key circuit with suitable teletypewriter security equipment.

i. Communications Security Development Programme

The Conference considers substantial economy of development resources on both sides of the Atlantic could be achieved if a directory were compiled showing the Combined and NATO communications security requirements and then a combined programme for communications security equipment were evolved from it.

The Conference recommends that the C.P.B. and N.S.A. should prepare such a directory and programme.

j. Exchange of equipments and components

The Conference recommends that as a regular procedure each nation provide to the other on an indefinite loan basis, for test and examination, engineering and first production models of components and equipments of mutual interest; and that if exchange is not practicable the equipment should be subjected to an agreed series of tests in the parent country.

k. Effects of advances in electronics

Advances in electronics and circuitry will have a profound effect upon crypto-operations, supply and maintenance as they are practised today. For this reason, thought and planning by the Services are required now if they are to be in a position to enjoy the full benefit of the advantages offered by electronic crypto equipments when they become available.

l. Co-ordination of Cryptographic and Communications Equipment Development

The present practice of almost independent development of cryptographic equipment and certain forms of communications equipment has at times led to incompatibility of one with the other. It is necessary that cryptographic equipment be designed to suit the requirements of the communications system or, where necessary, the communications equipment and practices be adjusted to make possible the utilisation of an acceptable cryptographic system.

The Conference recommends that the necessary steps be taken to ensure that such communications security as is required should be considered at the time when the Staff and Operational Specifications and/or Military Characteristics for communications equipment are being formulated.

m. Operating and Maintenance

The development authority must maintain close co-ordination with the user Services so that the operating and maintenance requirements are made known at all stages in the

development. Thus, users may weigh the need for the equipment against the maintenance and training requirements and, if necessary, the development authority may adjust the design to meet the operating and maintenance problem.

The Conference recommends that there be consultation between the development engineers and the engineers and communicators of the Services as early as possible in the process of development of each equipment in order to achieve these ends.

n. Standards of Security Requirements

During the Conference the U.K. and U.S. security advisers prepared an agreed method for the technical statement of security assessments of cryptosystems and the Services have adopted a method of expressing their security requirements; these will be of mutual assistance in deciding whether a proposed cryptosystem affords adequate security.

o. Future Liaison

(1) Working Staff. The Conference recommends that there should be an exchange, on a semi-permanent basis, of working cryptanalysts and engineers from the research and development establishments of the two nations; and that details should be worked out between CPB/GCHQ and NSA.

(2) Visits. The Conference recommends that the visits of engineers and security experts, independently of the Conferences, as already authorised (1952 Conference Report paragraph 11e) should continue.

6. Next Conference

The Conference recommends that the next Conference should be held in Washington in September/October, 1954, the programme to be agreed later in the light of developments in the meantime.

/s/ [redacted]
Major General,
for Chairman,
Cypher Policy Board.

/s/ W.F. Friedman,
Chairman,
U.S. Delegation.

~~TOP SECRET~~

COPY NO. 40

J.C.S. 2074/30

(LIMITED DISTRIBUTION)

12 February 1954

Pages 174 - 177, incl.

MEMORANDUM BY THE CHIEF OF STAFF, U.S. AIR FORCE

for the

JOINT CHIEFS OF STAFF

on

REPORT OF THE U.K./U.S. COMMUNICATION SECURITY CONFERENCE, 1953

Reference: J.C.S. 2074/29

CSAFM-27-54

1. I have examined J.C.S. 2074/29 and approve, with certain exceptions, the report of the 1953 Communications Security Conference. It appears to me that, in the interest of accuracy and clarity, the report in Enclosure "B" to J.C.S. 2074/29 must be changed as follows:

a. On pages 168 and 169, in subparagraph 5 a, lines 2 and 13 of the text should read "AFSAM-7/AFSAM 47-B" instead of "AFSAM 7" inasmuch as the same cryptographic principle is embodied in both of these machines. In line 2 the words "now in production in the U.S.A." should be deleted, since the AFSAM 47-B will not be in production until later this year.

b. On page 169, in subparagraph 5 e, delete all after the third line of the text inasmuch as the CAN-UK-US JCECs have not yet reached agreement on adopting multi-channel sub-carrier frequency modulation for the transmission of CIFAX.

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

c. On page 170, in subparagraph 5 f, second line, insert the word "military" between the words "unclassified" and "messages", in order clearly to isolate this problem from the problem of civil communications, which is essentially a matter of censorship.

d. On pages 170-1, in subparagraph 5 g, delete all after the seventh line of the text inasmuch as a discussion of the IFF Mark X system with SIF is not considered appropriate for inclusion in this report since the IFF Mark X system with SIF is neither cryptographic nor communication security equipment.

2. I recommend that:

a. The above changes to the report in Enclosure "B" to J.C.S. 2074/29 be approved and that the enclosed memorandum for the Representatives of the British Chiefs of Staff be forwarded in lieu of the draft memorandum in Enclosure "A" to J.C.S. 2074/29.

b. Upon receipt of concurrence from the British Chiefs of Staff, the changes set forth in paragraph 1 above be made to the report in Enclosure "B" to J.C.S. 2074/29.

E N C L O S U R E

D R A F T

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 U.K./U.S. Communication Security Conference, 1953. It is recommended that the subject report be changed as follows:

a. Paragraph 5 a, in the first and last sentences the term "AFSAM-7" should read "AFSAM-7/AFSAM 47-B", inasmuch as the same cryptographic principle is embodied in both of these machines. In line 2 the words "now in production in the U.S.A." should be deleted, since the AFSAM 47-B will not be in production until later this year.

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 adopting multi-channel sub-carrier frequency modulation for the transmission of CIFAX.

c. Paragraph 5 f, first sentence insert the word "military" between the words "unclassified" and "messages", in order clearly to isolate this problem from the problem of civil communications, which is essentially a matter of censorship.

d. Paragraph 5 g, delete all after the third sentence of the text, inasmuch as a discussion of the IFF Mark X system with SIF is not considered appropriate for inclusion in this report.

2. The United States Joint Chiefs of Staff wish to express their satisfaction with the results of the 1953 conference, especially the agreements reached on the problem of replacing

~~TOP SECRET~~

the existing combined and NATO High Grade off-line crypto-system. Every possible action is being taken to implement the replacement of this general cryptosystem.

3. 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~~

COPY NO. 40

J.C.S. 2074/31

(LIMITED DISTRIBUTION)

12 February 1954

Pages 178-179, incl.

NOTE BY THE SECRETARIES

to the

JOINT CHIEFS OF STAFF

on

REPORT OF THE U.K./U.S. COMMUNICATION SECURITY CONFERENCE, 1953

References: a. J.C.S. 2074/29
b. J.C.S. 2074/30

The enclosed memorandum by the Representatives of the British Chiefs of Staff, ACT 23, dated 9 February 1954, is hereby referred to the Armed Forces Security Agency Council for consideration in connection with the study directed by SM-128-54, dated 11 February 1954.*

EDWIN H. J. CARNS,
RICHARD H. PHILLIPS,
Joint Secretariat.

* See Note to Holders of J.C.S. 2074/29, dated 10 February 1954.

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

TOP SECRET

ENCLOSURE

BRITISH JOINT SERVICES MISSION

ACT 23
9th February 1954

THE SECRETARY,
UNITED STATES JOINT CHIEFS OF STAFF

U.K./U.S. Communications Security Conference, 1953

1. The U.K. Chiefs of Staff have approved the report of the U.K./U.S. Communications Security Conference 1953 (LCS(53)/P/R of 10th November, 1953*), and welcome the increase in the scope of the discussions as revealed therein.

2. They are aware of the complexity of many of the problems involved and of the present lack of a solution to meet some of the requirements. They are convinced however that these conferences are serving a very useful purpose and that material progress is being made towards greater security not only in Combined U.K./U.S. but also in NATO Communications.

/s/ A. C. TYLER,
Lieut. Colonel.

* Enclosure "B" to J.C.S. 2074/29.

~~TOP SECRET~~

TAB D

Recommended version of paragraph 5a of the Report (TAB A):

a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem*

The U.K. have accepted the U.S. cryptoprinciple embodied in the AFSAM 7 and AFSAM 4/B, of which the AFSAM 7 is now in production in the U.S.A. The new U.K. off-line machine, at present in the development stage, will embody this principle but as the U.K. machine is not expected to be in position before 1960, the U.S. will make available some 3,500 AFSAM 7 machines to the U.K. until the U.K. machine is available, and some 3,000 machines to other NATO countries, probably in time to introduce this system for Combined and NATO communications by 1st July, 1956. The U.K. and U.S. security experts have agreed that the security provided by the existing LUCIFER system (CCM) is acceptable in the meantime. The Conference recommends* that ultimately the cryptoprinciple embodied in the AFSAM 7 and AFSAM 4/B should be adopted for Combined and NATO third level use.

~~TOP SECRET~~

* Not added, underlined in original text.

TOP SECRET

TAB D

Recommended version of paragraph 5a of the Report (TAB A):

a. Replacement of the existing Combined and NATO High Grade off-line general cryptosystem*

The U.K. have accepted the U.S. cryptoprinciple embodied in the AFSAM 7 and AFSAM 47B, of which the AFSAM 7 is now in production in the U.S.A. The new U.K. off-line machine, at present in the development stage, will embody this principle but as the U.K. machine is not expected to be in position before 1960, the U.S. will make available some 3,500 AFSAM 7 machines to the U.K. until the U.K. machine is available, and some 3,000 machines to other NATO countries, probably in time to introduce this system for Combined and NATO communications by 1st July, 1956. The U.K. and U.S. security experts have agreed that the security provided by the existing LUCIFER system (CCM) is acceptable in the meantime. The Conference recommends* that ultimately the cryptoprinciple embodied in the AFSAM 7 and AFSAM 47B should be adopted for Combined and NATO third level use.

* Not added, underlined in original text.

TAB E

Recommended version of paragraph 5e of the Report (TAB A):

e. Facsimile security equipments (CIFAX)*

The U. K. and U.S. have specific projects for black/white CIFAX under test but it is as yet too early to consider one to meet Combined requirements.

The Conference recommends that the Communications Equipment Panel of the JCEGs be invited to agree a technical specification for a transmission system for Combined use with CIFAX.

As the CAN-UK-US JCEGs have already agreed that multi-channel sub-carrier frequency-modulation is the best method of transmission for CIFAX for other than short distance ground-wave HF radio links, the Conference recommends that the Communications-Equipment Panel of the JCEGs be invited to agree a technical specification for a multi-channel SCFM transmission system for Combined use with CIFAX.