~~TOP SECRET~~

Copy No. 8

LCS(53)/E/R

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Executive Committee

to

The Plenary Committee

1. The Executive Committee of the UK/US Communications Security Conference 1953 have completed their deliberations and have approved the detailed reports of the various Sub-Committees.

2. The Executive Committee have drafted a report on the Conference, including the major recommendations, and this is attached hereto.

3. It is recommended that

(a) The detailed Reports of the various Sub-Committees be submitted to the U.K. Cypher Policy Board and the U.S. National Security Agency for approval and further action as may be appropriate.

(b) The Enclosure be forwarded to the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff for approval.

[redacted] PL 86-36/50 USC 3605

Chairman,
Executive Committee

~~TOP SECRET~~

~~TOP SECRET~~

LCS(53)/P/R

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

~~TOP SECRET~~

844

TOP SECRET

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 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 JCFCs 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.

TOP SECRET

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.

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 to-day. 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.

~~TOP SECRET~~

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.

[redacted]
for Chairman,
Cypher Policy Board.

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

LONDON,
10th November, 1953.

~~TOP SECRET~~

~~TOP SECRET~~

Copy No. 3

LCS(53)/E/R(Draft)

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Executive Committee

to

The Plenary Committee

1. The Executive Committee of the UK/US Communications Security Conference 1953 have completed their deliberations and have approved the detailed reports of the various Sub-Committees.

2. The Executive Committee have drafted a report on the Conference, including the major recommendations, and this is attached hereto.

3. It is recommended that

(a) The detailed Reports of the various Sub-Committees be submitted to the U.K. Cypher Policy Board and the U.S. National Security Agency for information and further action as may be appropriate.

(b) The Enclosure be forwarded to the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff for approval.

[redacted]

PL 86-36/50 USC 3605

Chairman,
Executive Committee

~~TOP SECRET~~

~~TOP SECRET~~

LCS(53)/P/R (Draft).

Report

to the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff of the UK/US Communications Security Conference 1953.

1. In their endorsement of the Report of the UK/US Communications Security Conference which was held in Washington in May/June 1952 the U.K. Chiefs of Staff and the U.S. Joint Chiefs of Staff agreed that:

(a) The next Conference should be held in London in 1953.

(b) That a fortnight should be provided before the Conference opens for discussions between U.K. and U.S. Engineering and Security experts for examination of equipments and for visits to establishments.

(c) That the Conference itself should be in the following two phases, held concecutively:

(i) Phase I: Preparation by the Engineering and Security experts of Reports listing and assessing equipments available and under development.

(ii) Phase II: Meeting between U.K. and U.S. communications staffs and representatives of CPB and AFSAC to examine and define Combined and NATO operational requirements and, where possible, recommend equipments to meet them.

1. In accordance with the above, the 1953 Conference ~~opened~~ was held in London, ~~on 26th October and closed on 10th November.~~ 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.

~~TOP SECRET~~

~~TOP SECRET~~

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.

5. Reports of the various Committees which discussed the items listed in paragraph 2 above have been submitted to the U.K. Cypher Policy Board and the U.S. National Security Agency for information and further action as may be appropriate ~~on the principal points mentioned below~~.

3. The Conference included a full and frank exchange of views on all the items listed, 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 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. ~~ADONIS~~ cryptoprinciple now in production in the U.S.A. ~~as AFSAM 7~~. 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 to the U.K. ~~on free loan~~ until the U.K. machine is available, some 3,500 AFSAM 7 machines, probably in time to introduce this system for Combined and NATO communications by 1st July, 1956. The U.K. and U.S. security /experts

~~TOP SECRET~~

experts have agreed that the security provided by the existing LUCIFER system (CCM) is acceptable in the meantime. The U.K. and U.S. also recommend that, ultimately, ~~the ADONIS cryptosystem~~ the cryptoprinciple embodied in the AFSAM-7 should be adopted for Combined and NATO ~~low echelon~~ third-level use.

(b) Low echelon off-line cypher machine, without external power supply.

The U.K. and the U.S. agree that there is a [major] requirement for a machine requiring no ~~external~~ electrical power supply for Combined and NATO ~~low echelon~~ third-level use [by the Navies and Air Forces]. There is no machine presently available which will meet this requirement but the D.17 now under development by the U.S. may provide a possible ultimate solution.

(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 ~~systems~~ equipments in existence and others are in course of development. ~~At the moment, none are capable of interworking, owing to independent design and it is necessary for one nation to equip both terminals of any international link.~~ 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 U.K. and the U.S. agree that radiation, conduction and induction from communication and crypto devices are ~~a serious~~ 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 [Service].

/f)

(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 distances ground-wave HF radio links, it is recommended 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.

(g) Non-machine off-line cryptosystems, including Combat and special purpose systems.

The Conference reviewed the multiplicity of requirements for hand systems for combat and special purposes and re-affirmed its concern at the lack of security and speed which have to be accepted, due to there being no suitable machine system available at present.

(f) Transmission security.

The Conference was greatly concerned that unclassified messages originated by Service authorities in peace time are transmitted in plain language by insecure means. Such messages not only lead to the relevation 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

The ~~U.K. and U.S.~~ Conference recommends that ~~each should set up~~ small Working Groups of security advisers and users 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.

(c) 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, it is recommended 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 J.C.E.C.'s be invited to restate the security requirements for a system to operate in conjunction with I.F.F. Mk. 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 J.C.E.C.'s the cryptographic agencies of the U.S. and the U.K. make joint technical proposals for a new and secure I.F.F. system ~~on the following basis:-~~

(a) That if possible it should be compatible with the Mark X transponder unit.

(b) That if (a) above is found to be impossible they should, in conjunction with the appropriate communications agencies, recommend development of a new system providing the required security. This system might have to be integrated with its own transponder if this is deemed advisable.

(h) Weather cryptosystems.

The U.K. and U.S. have agreed that the CCM should be adopted as the off-line machine system requested in the NATO Meteorological Plan and it is recommended 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. It is appreciated that not all the on-line teletypewriter security equipment asked for can be supplied by that date but very early provision should be made to equip the New York/Azores/Paris and Port Lyautey service with suitable machines in an emergency.

Should an emergency arise before 1st May, 1954, the U.K. can immediately offer sufficient quantities of their Meteorological Stencil Subtractor Frame system for rapid distribution to NATO until the C.C.M. is available.

(i) ~~Engineering.~~ C/S Program.

~~It~~ It is thought that considerable economy of development resources on both sides of the Atlantic could be achieved if a ~~directory were~~ Combined program ~~compiled showing~~ C/S devs. were to be prepared. This program should include the Combined and NATO communications security requirements ~~and which cryptographic equipments or systems should be selected to meet them.~~

A program etc

It is intended to invite the ~~CAN-UK-US J.C.E.C.'s to compile~~ such a directory.

/(2)

~~TOP SECRET~~

(a) Exchange of Equipment & Components

(7) It is recommended 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.

(b) Effects of advances in electronics

(8) ~~There have been significant advances in electronics and circuitry since the 1952 Conference.~~ These will have a profound effect upon crypto-operations, supply and maintenance as they are practised to-day. For this reason, thought and planning ~~should be started now~~ by all users of the Services 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.

(c) 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 ~~usually~~ at times led to incompatibility of one with the other. In order that compatibility may be achieved it ~~is~~ essential that such communications security as is required should be considered ~~an integral part of the communications equipment~~ at the time when the Staff and Operational ~~Specifications and/or Military Characteristics are being formulated.~~ This is necessary ~~so~~ that the cryptographic equipment may be designed to suit the requirements of the communications system or, where necessary, the communications equipment and practices may be adjusted to make possible the utilisation of an acceptable cryptographic system.

It is recommended that the necessary steps be taken to ensure that ~~this~~ course of action is ~~adopted by all concerned.~~

/Operating

~~TOP SECRET~~

(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.~~

It is recommended that there be consultation between the development engineers and the Service engineers and communicators 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. It is recommended 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. It is recommended that the visits of engineers and security experts, independently of the Conferences, as already authorised (1952 Conference Report paragraph 11 e) should continue.

TOP SECRET

6. Next Conference.

It is recommended:

That the next Conference should be held in Washington in 1954, in two phases to be conducted consecutively as follows:- the program for the Conference to be agreed later in the light of developments made in the meantime:

Phase I. Engineers and Operational Communicators of the Service Departments, Development Engineers with such security advisers from NSA and CPB/GCHQ as may be appropriate to inspect and discuss equipments.

Phase II. Operational Communicators from the Service Departments and representatives of C.P.B. and N.S.A. to define Combined and NATO Operational requirements and, where possible, to recommend equipments to meet them.

PL 86-36/50 USC 3605

[redacted]
Chairman,
Cypher Policy Board.

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

TOP SECRET