844

U.S.

~~TOP SECRET~~ FROTH

Copy No. 1

LCS(53)/S/Report (Final Draft).

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

REPORT OF THE SECURITY SUB-COMMITTEE

to the

EXECUTIVE COMMITTEE

1. The Security Sub-Committee has made security assessments of U.K. and U.S. systems which are attached at Appendix A. It should be noted that the phrase "further study required" as applied to an equipment still under development means that information is insufficient for a final assessment but that continued development is justified.

2. Recommendations on transmission security are attached at Appendix B.

3. An agreed method of expressing security assessments is attached at Appendix C, together with proposals for the information which should be provided by users in stating their requirements from the security point of view. Because of the nature of the discussion in this paper the Security Sub-Committee recommends that only the following statement be included in the main report of the Conference:

> "During the Conference the U.K. and U.S. security advisers prepared an agreed method for the technical statement of security assessments."

4. In addition the Security Committee has the following general recommendations to make:-

a. A high priority should be given to a thorough investigation of:

(1) the properties of quantised speech;

(2) the practicability of intercepting, recording and counting the output of many of the speech equipments under consideration.

b. Steps should be taken to replace as soon as possible equipments employing an additive system in such a way that there is a significant danger of producing a readable depth of two.

/c.

c. Only one-time key tape which has been produced and checked in accordance with agreed UK/US standards should be employed with one-time tape equipments.

d. All equipments should be rendered secure against spurious emissions which endanger communications security.

e. The design of on-line equipments should be such that it is impossible to transmit plain text inadvertently in place of cypher text.

f. Further study should be made of keyboard operation with start/stop on-line teleprinter cyphering systems to analyse the dangers arising from operator and machine idiosyncracies.

g. The cypher signal transmitted from an on-line cypher system must be a pure cypher signal not containing any elements recognisable as plain text or cypher key.

h. The cognisant authorities should be informed of the UK/US views on the security of the S.I.F. with I.F.F. Mark X. If a solution to this problem is to be found it is essential that the users should state their overall security requirements for an I.F.F. system.

5. The Security Sub-Committee also offers the following recommendations to improve security liaison between ~~N.S.A.~~ and GCHQ/CPB.

a. An exchange of working cryptanalysts between N.S.A. 41 and G.C.H.Q. [redacted] the details to be worked out between N.S.A. and G.C.H.Q.

PL 86-36/50 USC 3605

~~b.~~ In addition to this exchange of personnel, ~~frequent~~ visits between U.K. and U.S. for ~~thorough~~ technical discussions of communications security ~~these would replace the informal talks and Phase I stages of future COMSEC Conferences but should not preclude the presence of security advisors at future Phase II type Conferences.~~

/c.

844

b. A more rapid interchange of new information and ideas affecting systems under assessment and questions of transmission security.

c. The preparation of an agreed programme of cryptographic assessments for the coming year; this programme to include both U.K. and U.S. systems which require assessment; N.S.A. 41 to prepare a draft programme of this kind and forward to the C.P.B. for agreement.

[redacted] PL 86-36/50 USC 3605

Chairman
Security Sub-Committee (Phase I)

3rd November, 1953.

TOP SECRET

Copy No. [redacted] 1

APPENDIX 'A' to the Report of the Security Sub-Committee to the Executive Committee.

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

SECURITY ASSESSMENT OF CRYPTOGRAPHIC EQUIPMENTS IN USE AND UNDER DEVELOPMENT

1. Off-line Equipments including Teletypewriter Equipment used off-line.

2. On-line Teletypewriter Systems.

3. Speech and Cifax Equipments.

4. Special Purpose and Hand Systems.

5. Cryptographic Production Equipments.

30th October, 1953.

TOP SECRET

1. Off-line Equipments: Teletypewriter Equipment used Off-line: Special Purpose System

a. U.S. Equipments

(1) AFSAM D.17

(a) The U.K. require further study.

(b) The U.S. consider that with clear indicators the system is secure for low echelon traffic.

(2) AFSAM D.21

The U.K. and U.S. consider that the equipment is secure subject to adequate checks of the standard of the one-time key tapes.

(3) AFSAM 36

(a) The U.K. consider that with adequate precautions in the choice of machine set-up, with bisection and with message lengths restricted to 250 letters the system is adequately secure for low echelon use.

(b) The U.S. consider, that with the limitations already placed on it, the machine is adequately secure as a low ecelon system but they will examine the U.K. limitations in detail.

(4) AFSAM 7

(a) POLLUX

(i) The U.K. are not in favour of clear indicators because of the possibility of recognising and exploiting tailing messages and messages in depth. Further study required when more is known about traffic loads and the likelihood of operators' errors.

(ii) The U.S. consider the system adequately secure for low echelon use but they will keep traffic under review. If dangerous insecurities appear they feel that they can modify the procedures sufficiently to overcome them.

(b) ADONIS

(i) The U.K. consider that ADONIS is secure for all classifications of traffic for at least the next ten years provided that a good standard of operating is maintained but require further study in view of the recent increase in the number of elements.

/(ii)

(ii) The U.S. consider that ADONIS is secure for all classifications of traffic for the next twenty years provided that a good standard of operating is maintained.

(5) AFSAM 47 (BRUTUS)

The U.K. and U.S. consider that the system is secure for all classifications of traffic for at least the next five years provided that a good standard of operating is maintained.

(6) CSP 888/889 (HERCULES)

The U.K. and U.S. agree that the HERCULES system is secure for all classifications of traffic for the next five years provided a good standard of operating is maintained.

(7) C.C.M. (LUCIFER)

(a) The U.K. and U.S. agree that LUCIFER gives adequate security for all classifications of traffic for not more than three years provided that a good standard of operation is maintained, but consider that the C.C.M. must be replaced as soon as possible.

(b) For Meteorological traffic, the U.K. and U.S. agree

(i) that it is not essential to have separate rotors for meteorological messages provided that there are separate key lists.

(ii) that in ship-to-shore systems short meteorological messages can be incorporated in ordinary messages.

(8) SIGTOT (Off-line use)

The U.K. and U.S. agree that the system is secure for all classifications of traffic subject to adequate checks of the standard of the one-time key tape and provided that effective physical methods are employed to prevent the re-use of key tape.

(9) ASAM 2-1 (ORCUS)

(a) The U.K. believe that the indicator system may be vulnerable and if this is so the machine set-up for each link using the same key pad can be recovered. Further study is required when details of traffic volume and message lengths are available.

(b) The U.S. believe that the volume of traffic encyphered on one machine is too little to make this a serious shortcoming but also requires further study.

/(c)

(c) The U.K. and U.S. are concerned however at the insecurities which may arise as a result of operator's errors and agree that the procedure, being one which permits of a significant danger of producing a readable depth of two, should be replaced.

(d) The U.K. and U.S. agree that the machine should be replaced as soon as possible.

b. U.K. Equipments

(1) PORTEX

(a) The U.K. regard the system as adequately secure for low echelon use for the next fifteen years provided that

(i) the number of groups encyphered at each indicator is limited to 50 groups,

and (ii) indicators are extracted from specially constructed key lists.

For higher level use indicators must be disguised (encyphered) and messages limited to 50 groups. Even so, if it is necessary to legislate for the undisciplined operator PORTEX cannot be guaranteed as adequate for TOP SECRET traffic for more than the next five years. If the rules are observed and assuming an adequate indicator system, the machine may be regarded as secure for the next twenty years. The U.K. consider PORTEX to be a Category 'A' cryptosystem.

(b) The U.S. require further study.

(2) TYPEX II. (SIMPLEX)

The U.K. and U.S. agree that the system can be regarded as adequately secure for the next five years for all classifications of traffic provided that

(a) a good standard of operating is maintained,

(b) bisection procedure is used,

(c) the variable spacing used is of the 1, 2, 3 type.

(3) TYPEX MARK 22

(a) The U.K. consider the equipment is secure for all classifications of traffic for at least the next five years.

(b) The U.S. know nothing against the system but require further study.

/(4)

(4) SINGLET/PENDRAGON/COPPERFIELD (UPSTART)

The U.K. and U.S. know nothing against the system but require further study.

(5) ROCKEX

The U.K. and U.S. agree that the system when used correctly is secure for all classifications of traffic subject to adequate checks of the standard of one-time key tape and to further study of spurious emissions which endanger communications security.

c. Miscellaneous Equipments

(1) [redacted]

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

(a) [redacted] Adequate security for low echelon use could be achieved by the use of a codebook provided that no spaces are encrypted between groups.

(b) The U.S. require further study as a matter of urgency in view of the U.K. statement.

(2) CX-52 and CX-52H

The U.K. and U.S. require further study as a matter of urgency but there seems little doubt that it will give a very high degree of security if properly used.

2. On-line Teletypewriter Systems

a. U.S. Equipments

(1) AFSAM 9/AFSAZ D7315

(a) ATHENA

The U.K. are not in favour of the use of clear indicators.

The U.S. require further study as to the extent to which clear indicators can be used on higher level nets but consider that clear indicators are probably acceptable on low echelon nets.

The U.K. would approve the use of AFSAM 9 with AFSAM 109 with encyphered indicators for all classifications of traffic for the next five years provided a reasonable standard of operating is maintained. During the period a very careful investigation should be made of the occurrence of operators' errors. If operators' mistakes are such that any of the attacks appear dangerous the U.K. suggests that the machine be modified by the addition of a plugboard.

/(b)

(b) AENEAS

The U.K. and U.S. agree that the system is secure for all classifications of traffic subject to adequate checks of the standard of the one-time key tape.

(c) PYGMALION/IRIS

(i) The U.K. view is the same as in the case of AFSAM 9 with AFSAM 109 with encyphered indicators but they are also concerned about the loss of traffic flow security if indicators are chosen at random.

(ii) The U.S. consider the systems will be secure for all classifications of traffic if properly used, but after experience of the machine under operational conditions they may have to revise the procedures. They consider that operators' errors can prejudice security but they do not expect them to occur sufficiently frequently for there to be any danger of compromise.

(2) ASAM 2-1 (DAPHNE)

(a) The U.K. and U.S. agree that DAPHNE procedure is adequate for on-line or off-line use. The achievement of security of traffic passed by DAPHNE procedure requires the modification of the associated equipment, where necessary, to eliminate the possibility of operators' faults which may cause inadvertent transmission of plain text.

(b) U.K. and U.S. agree that the machine should be replaced as soon as possible.

(3) AFSAM 4A (CENTAUR and IXION)

(a) U.K. require further study.

(b) U.S. accept CENTAUR and IXION procedures but will review the indicator procedure for certain uses.

(4) AFSAM 44, AFSAM 45

U.K. and U.S. agree that the system is secure for all classifications of traffic subject to adequate checks of the standard of the one-time key tape.

(5) SIGTOT

U.K. and U.S. agree that the system is secure for all classifications of traffic subject to adequate checks of the standard of the one-time key tape and subject to a modification of the associated equipment to prevent inadvertent transmission of the plain text.

/(6)

(6) AFSAM D.22

(a) The U.S. consider the machine secure for all classifications of traffic.

(b) The U.K. require further study. Nothing known against.

(7) AFSAM D.26

U.K. and U.S. require further study.

(8) AFSAM D.37

U.K. and U.S. require further study.

b. U.K. Equipments

(1) MINSTER

U.K. and U.S. noted that the U.K. Services do not intend to use this equipment.

(2) METROPOLE

U.K. and U.S. require further study.

(3) PHILOMEL

U.K. and U.S. require further study.

(4) CONVERTOR NO. 5

U.K. and U.S. agree that the equipment, when used with Apparatus 5 U.C.O., provides adequate security for all classifications of traffic for the next twenty years. It is believed that complete traffic flow security will be provided; further study will be made to verify this.

(5) ARTICHOKE

U.K. and U.S. agree that the equipment provides adequate security for all classifications of traffic for the next twenty years. It is believed that complete traffic flow security will be provided; further study will be made to verify this.

(6) APPARATUS 5 UCO

U.K. and U.S. agree that subject to adequate checks of the standard of one-time key tape the equipment is secure for all classifications of traffic.

(7) CIRCUIT MERCURY

U.K. and U.S. agree that the equipment is secure for all classifications of traffic for at least the next twenty years.

/(8)

(8) INCUBATOR

U.K. and U.S. require further study.

3. Speech and Cifax Equipments

a. U.S. Equipments

(1) AFSAY D.806

(a) The U.S. consider the system is secure for at least the next five years.

(b) The U.K. require further study, since the number of variables in the system has been increased.

(2) AFSAY D.809

U.K. and U.S. require further study.

(3) AFSAY D.807

(a) U.K. consider that if D.807 transmissions can be intercepted and recorded, the machine cannot be regarded as secure for SECRET traffic. The technical difficulties of interception and recording are at present so great that they add considerably to the security of the system.

(b) U.S. consider the machine secure for all classifications of traffic subject to further investigation of the possibility of intercepting and recording or counting.

(4) AFSAY D.808

U.K. and U.S. require further study.

(5) AFSAY D.810

U.K. and U.S. require further study.

(6) AFSAY D.816

(a) U.K. consider that if D.816 transmissions can be intercepted and counted, the equipments cannot be regarded as secure even for Secret traffic.

(b) U.S. require further study of U.K. views.

(7) AFSAY D.801

U.K. and U.S. require further study.

/(8)

(8) AFSAY D.804

(a) The U.K. view is that the system without random walk rings cannot be considered to provide the degree of security required. Further study of systems with random walk rings is required.

(b) The U.S. consider that the system without random walk rings but with appropriate alarms is secure for low echelon use although they recognise the possibility of successful high speed attack. The U.S. consider that the system with random walk rings and alarms is secure for all classifications of traffic.

(9) AFSAY D.830

U.K. and U.S. agree that the system is not secure and do not recommend its use for any purpose.

(10) AFSAJ 700

The U.K. and U.S. agree that the equipment is secure for on-line encypherment of facsimile or teletype for at least the next twenty years. The U.S. will carry out experiments to verify that adequate traffic flow security will be provided in multi-channel teletypewriter use.

(11) AFSAX 503

U.K. and U.S. agree that the equipment is secure for all classifications of traffic for the next twenty years.

(12) AFSAX D.505

U.K. and U.S. require further study.

b. U.K. Equipments

(1) BANGLE

(a) U.K. and U.S. agree that the equipment is secure for all classifications of traffic subject to adequate checks of the key film and provision of satisfactory alarms.

(2) SORCERER

U.K. and U.S. agree that the equipment is secure for all classifications of traffic for the next twenty years.

(3) BLUE BOY (D.70)

(a) The U.K. view is that because of practical difficulties of intercepting and recording, the Apparatus D.70 which includes the key generator BLUE BOY, may be considered as secure for a period of at least five years. It is still under study.

/(b)

(b) The U.S. require further study.

(4) TRUMPETER

U.K. and U.S. require further study.

(5) HALLMARK II

U.K. and U.S. require further study. More experimental data on the properties of speech in delta modulation systems are required before a final assessment can be made.

(6) PICKWICK

U.K. and U.S. require further study.

(7) MOUNTEBANK

(a) U.K. consider the equipment is secure for the next twenty years.

(b) U.S. require further study. Nothing known against.

4. Special Purpose Systems

a. AFSAM 499

U.K. and U.S. require further study in the light of the possibility of planned interrogation by an enemy.

b. AFSAM 498

The U.K. and U.S. agree that the machine is theoretically not secure against planned interrogation by an enemy.

c. AFSAM D.31

The U.K. and U.S. agree that the system is secure subject to adequate checks of the standard of the one-time key tape.

d. NATEX

(1) Security

(a) The U.K. consider that with the restrictions already suggested by them the NATEX cryptosystem with underlying plain text is adequately secure for all classifications of traffic but there is some danger from cribs and operators' errors.

(b) The U.S. consider that NATEX with underlying plain text is secure as long as certain restrictions are imposed, but require further study on the exact nature of the restrictions.

/(c)

(c) The U.K. and U.S. agree that the use of an underlying codebook would have considerable security advantages and make some of the restrictions unnecessary.

(2) Indicators

(a) The U.K. and U.S. agree that for general NATEX use it is desirable to have a new five letter indicator system which would enable the message to start at any position on the line.

(b) The U.K. and U.S. agree that the indicator system proposed by the U.S. be recommended for NATEX 3rd level use with the following modifications:

(i) identification of the indicator page to be from message externals only,

(ii) operators to be forbidden to choose the six letter indicators from their assigned page in regular order.

e. Running Key Cypher (U.S. MERCURY)

(1) The U.K. consider that if plain language basic text is used with R.K.C. in quantity or with any regularity the system is not secure. Provided, however, that a well constructed basic book is used, security is greatly improved, but it cannot be guaranteed that exploitation of an occasional key table will never be possible. The U.K. consider R.K.C. to be a Category B system.

(2) The U.S. generally agree but require to study further the U.K. views particularly on the Category. It is now in existence as a Category 'A' system.

f. GRIP

The U.K. and U.S. agree that the system is not secure and do not recommend its use for any purpose.

g. Double Subtraction on S.S. Frame

The U.K. and U.S. agree that the system is secure for all classifications of traffic provided that different key sheets are used for the two subtractions and that the agreed safe traffic load is not exceeded.

h. I.F.F. System (High Security Identification)

(1) the U.K. require study.

(2) The U.S. consider that the system is marginally secure but it can be improved by the addition of another permutation.

i. S.I.F. with I.F.F. Mark X

(1) Mode 1

The only cryptographic features of S.I.F. with I.F.F. Mark X are the methods proposed for providing the changing codes in Mode 1 operation. Even if the methods of changing the code were

/cryptographically

cryptographically secure, the U.K. and U.S. agree that it is not possible to change the code frequently enough to prevent the enemy from masquerading. In addition, the risk of physical compromise of the cryptographic element is great. The U.K. and U.S. therefore agree that the use of S.I.F. with I.F.F. Mark X on Mode 1 with or without any code changer is an insecure method of proving an identity.

(2) Modes 2 and 3

No cryptographic security is proposed for Mode 2 and 3 use of S.I.F. with I.F.F. Mark X and the U.K. and U.S. agree that these functional and personal identity modes could be a most valuable source of intelligence to the enemy.

(3) For the reasons given above the U.K. and U.S. agree that the whole of the present programme for the use of S.I.F. with I.F.F. Mark X should be reconsidered.

5. Cryptographic Production Equipments

a. AFSAW 7200

The U.K. and U.S. agree that subject to satisfactory results from zero increment counts and from all standard checks on individual tapes, the tapes produced by AFSAW 7200 can be considered adequate for all types of use.

U.K. Equipments

b. 5 UCO Key Generator

The U.K. and U.S. agree that subject to adequate checks during and after production the tape produced by the equipment is secure.

c. ROCKEX Key Generator

The U.K. and U.S. agree that subject to adequate checks during and after production the tape produced by the equipment is secure.

d. BANGLE Key Generator

The U.K. and U.S. agree that the key film is probably secure but further study is required because of a small bias which has been detected in the key film generator.

e. TRIMMER

The U.K. and U.S. agree that further study is required but, subject to adequate checks of the output, the key produced is probably secure.

/f.

f. U.K. HOLLERITH Methods

U.K. and U.S. agree that pads produced by this method are secure provided that adequate supervision is maintained during production.

g. U.S. Pad Production Method

U.K. require study

U.S. consider that pads produced by this method are secure.

NOTE: A check of a production equipment or its product is considered adequate if the check is designed to meet agreed UK/US criteria.

844

~~TOP SECRET~~

APPENDIX B to the report of the Security Sub-Committee to the Executive Committee.

COPY NO: 1

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953.

SECURITY SUB-COMMITTEE
REPORT ON TRANSMISSION SECURITY

1. Present Situation.

The U.K. and U.S. agree that British and U.S. measures to maintain transmission security do not reach the same standard of efficacy as do those for the maintenance of cryptographic security. Present practices are insufficient to deny a potential enemy intelligence derived from the study of elements of transmissions external to the cypher text.

2. Contributory Factors.

There are a number of inter-related communications practices and methods which contribute to this state of insecurity; these are discussed below:

a. The Use of Plain Language.

The use of plain language for the transmission of messages, even those in themselves unclassified, not only leads to revelation of intelligence but tends 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 jeopardize the security of the latter and of the address procedures employed with them. The U.K. and U.S. agree that radio transmission of plain language messages should be forbidden, regardless of whether classified or not, excepting cases covered by the already agreed proviso that in tactical situations, ~~the commanding officer may authorize the sending of messages in the clear.~~

b. The Use of Plain Language Addressing on Encrypted Messages.

The use of plain language addressing on encrypted messages leads to provision of direct intelligence of the order of battle type and also to possibilities of assuming with fair accuracy the content of certain of the encrypted messages so headed. The U.K. and U.S. agree that the use of

/plain

~~TOP SECRET~~

plain language addressing on classified messages should be abolished.

c. Call Signs.

Call Sign Systems used by all stations other than the large fixed ones which must inevitably be identifiable, must be secure against the enemy tracing the continuity of identity from day to day. At present there is no universal means for providing this call sign security although there is agreement on the use of daily changing call signs in time of war. The U.K. and U.S. have examined the basic call sign systems and the "call sign encryption plan" and agree the following:

(1) Daily changing calls should be instituted in time of peace. Their value lies not only in the intelligence they deny the enemy but in making harder or impossible his task of maintaining continuity of identification from peace to war.

(2) New basic books should be produced and should be compiled with properly hatted variants.

(3) The use of a common call sign encryption key list for all Services world-wide has considerable security disadvantages.

(4) The overall adequacy of the current system for the encryption of call signs should be reinvestigated and if necessary a new one devised. Any new system for call sign encryption, in addition to being secure, even with the basic bock compromised, must be easy to use and to produce.

d. Frequency Changing.

The U.K. and U.S. agree a means must be found to change frequencies at a rapid rate and with wide variations; that failure to do this will tend to diminish the security achievable by the other practices under discussion.

e. External Characteristics of Cryptosystems.

The U.K. and U.S. agree that the fact that cryptosystems can be sorted into general types by external characteristics, and into specific types by system indicators (discriminants) is a source of insecurity that should be eliminated. /f.

f. Authentication.

The U.K. and U.S. agree that the currently approved systems and methods for authentication, although secure in many respects, do not in fact afford a guarantee of the authenticity of transmissions or a positive safeguard against intrusion.

g. Message Externals in Tape Relay.

Present tape relay systems cannot operate without undisguised routing indicators. The U.K. and U.S. agree that undisguised routing indicators provide valuable intelligence and that their ~~use~~ transmission over radio and sensitive line circuits must be eliminated. ~~Therefore, present tape relay procedures require a basic overhaul.~~ The U.K. and U.S. agree that ~~the most feasible alternative~~ an effective method appears to be the adoption of total link encryption on radio & sensitive land line circuits using cryptosystems capable of providing "automatic traffic flow security". The U.K. and U.S. have agreed the following definition of this term:

"Automatic traffic flow security is the condition achieved by automatic means, in which an enemy is denied knowledge of the volume and routing of traffic passed over a circuit".

Thus automatic traffic flow security not only disguises message externals but also prevents traffic analyses based on total volume and message lengths.

3. Recommendations.

a. The U.K. and U.S. fully realise that proper implementation of the above constitutes an ideal, but agree that serious and urgent consideration be given to the determination of the maximum degree of transmission security which can be achieved. They accordingly recommend that small Working Groups consisting of security advisors and users should be set up on both sides of the Atlantic to study the problems & provide a solution ~~to the problem.~~ The results should be exchanged between the U.K. and U.S. and on the basis of these combined plans made. Although no limit should be placed on the terms of reference of these groups in the field of transmission security, it is felt that the following list includes those items on which immediate action is possible:

/(1)

844

~~TOP SECRET~~

(1) New basic call sign books should be prepared using variants compiled in accordance with criteria provided by NSA (U.S. action)

(2) Agreement should be reached on the practicability of using a number of call sign encryption key lists in lieu of a single world wide key.

(3) Study of and recommendations regarding replacement of the current call sign encryption system, based at least in part on the evidence produced by Exercise MARINER.

(4) The following data with regard to authentication should be provided:

(1) Types of authentication for which systems are required.

(2) Degree of protection needed.

(3) Chances and scope of planned interrogation by an enemy.

b. The aforementioned working groups should consider the remaining questions of plain language, plain language headings, frequency changing, message externals in tape relay, together with any other associated items as rapidly as possible.

c. N.S.A. and C.F.B. should evaluate methods for providing all cryptosystems within a class with identical external characteristics. Special attention should be given to a means for eliminating the use of undisguised system indicators in messages passed in the cryptosystem chosen to replace CCM.

3rd November, 1953.

~~TOP SECRET~~

~~TOP SECRET~~

APPENDIX B to the report of the Security Sub-Committee to the Executive Committee.

Copy no. 4.

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953.

SECURITY SUB-COMMITTEE
REPORT ON TRANSMISSION SECURITY

1. Present Situation.

The U.K. and U.S. agree that British and U.S. measures to maintain transmission security do not reach the same standard of efficacy as do those for the maintenance of cryptographic security. Present practices are insufficient to deny a potential enemy intelligence derived from the study of elements of transmissions external to the cypher text.

2. Contributory Factors.

There are a number of inter-related communications practices and methods which contribute to this state of insecurity; these are discussed below:

a. The Use of Plain Language.

The use of plain language for the transmission of messages, even those in themselves unclassified, not only leads to revelation of intelligence but tends 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 jeopardize the security of the latter and of the address procedures employed with them. The U.K. and U.S. agree that radio transmission of plain language messages should be forbidden, regardless of whether classified or not, excepting cases covered by the already agreed proviso that in tactical situations the commanding officer may authorize the sending of messages by radio in the clear.

b. The Use of Plain Language Addressing on Encrypted Messages.

The use of plain language addressing on encrypted messages leads to provision of direct intelligence of the order of battle type and also to possibilities of assuming with fair accuracy the content of certain of the encrypted messages so headed. The U.K. and U.S. agree that the use of plain language addressing on classified messages should be abolished.

c. Call Signs.

Call Sign Systems used by all stations other than the large fixed ones which must inevitably be identifiable, must be secure against the enemy tracing the continuity of identity from day to day. At present there is no universal means for providing this call sign security although there is agreement on the use of daily changing call signs in time of war. The U.K. and U.S. have examined the basic call sign systems and the "call sign encryption plan" and agree the following:

(1) Daily changing calls should be instituted in time of peace. Their value lies not only in the intelligence they deny the enemy but in making harder or impossible his task of maintaining continuity of identification from peace to war.

(2) New basic books should be produced and should be compiled with properly hatted variants.

(3) The use of a common call sign encryption key list for all Services world-wide has considerable security disadvantages.

(4) The overall adequacy of the current system for the encryption of call signs should be reinvestigated and if necessary a new one devised. Any new system for call sign encryption, in addition to being secure, even with the basic book compromised, must be easy to use and to produce.

d. Frequency Changing.

The U.K. and U.S. agree a means must be found to change frequencies at a rapid rate and with wide variations; that failure to do this will tend to diminish the security achievable by the other practices under discussion.

e. External Characteristics of Cryptosystems.

The U.K. and U.S. agree that the fact that cryptosystems can be sorted into general types by external characteristics, and into specific types by system indicators (discriminants) is a source of insecurity that should be eliminated. /f.

f. Authentication.

The U.K. and U.S. agree that the currently approved systems and methods for authentication, although secure in many respects, do not in fact afford a guarantee of the authenticity of transmissions or a positive safeguard against intrusion.

g. Message Externals in Tape Relay.

Present tape relay systems cannot operate without undisguised routing indicators. The U.K. and U.S. agree that undisguised routing indicators provide valuable intelligence and that their radio transmission over radio and sensitive line circuits must be eliminated. Therefore, present tape relay procedures require a basic overhaul. The U.K. and U.S. agree that the most feasible alternative appears to be the adoption of total link encryption using cryptosystems capable of providing "automatic traffic flow security". The U.K. and U.S. have agreed the following definition of this term:

"Automatic traffic flow security is the condition achieved by automatic means, in which an enemy is denied knowledge of the volume and routing of traffic passed over a circuit."

Thus automatic traffic flow security not only disguises message externals but also prevents traffic analyses based on total volume and message lengths.

3. Recommendations.

a. The U.K. and U.S. fully realise that proper implementation of the above constitutes an ideal, but agree that serious and urgent consideration ~~may~~ should be given to ~~them~~ the determination of the maximum degree of transmission security which can be achieved. They accordingly recommend that ~~the~~ small Working Groups consisting of security advisors and users should be set up on both sides of the Atlantic to provide a solution to the problem. The results should be exchanged between the U.K. and U.S. and on the basis of these combined plans made. Although no limit should be placed on the terms of reference of these groups in the field of transmission security, it is felt that the following list includes those items on which immediate action is possible: /(1)

(1) New basic call sign books should be prepared using variants compiled in accordance with criteria provided by NSA (U.S. action)

(2) Agreement should be reached on the practicability of using a number of call sign encryption key lists in lieu of a single world wide key.

(3) Study of and recommendations regarding replacement of the current call sign encryption system, based at least in part on the evidence produced by exercise MARINER.

(4) The following data with regard to authentication should be provided:

(1) Types of authentication for which systems are required.

(2) Degree of protection needed.

(3) Chances and scope of planned interrogation.

b. The aforementioned working groups should consider the remaining questions of plain language, plain language headings, frequency changing, message externals in tape relay, together with any other associated items as rapidly as possible.

c. N.S.A. and C.C.B. should evalue methods for providing all cryptosystems within a class with identical external characteristics. Special attention should be given to a means for eliminating the use of undisguised system indicators in messages passed in the cryptosystem chosen to replace CCM.

TOP SECRET

TO BE HANDLED IN ACCORDANCE WITH IRSIG

FROTH

Copy No: 1

[redacted]

/3.

It seems that analogs of rotor machines will tend to be slower and costlier than analogs of electronic devices. It is extremely difficult however to say how much slower and costlier, since operations vary widely, and unexpected

ANNEX B to Appendix C
LCS(53)/S/Report (Final Draft)

Expression of Security Requirements

Considerations Relevant to the Problem

1. In order to make an assessment the security advisers require to know at least:-

   a. the degree of confidence to be placed in the system (the Confidence Factor)

   b. the proposed level of use

   c. the expected traffic load

   d. the minimum acceptable message length

   e. details of any special traffic peculiarities.

2. Provision of the information required under 1b to 1e above presents little difficulty but determination of the Confidence Factor is not so straightforward. The Confidence Factor may be defined as the tolerable expected proportion of unreadable messages to readable messages within a stated period of time. In calculating the acceptable Confidence Factor it will be necessary to take the following factors into account:-

   a. the classification of traffic to be passed in the system

   b. the Intelligence importance of the traffic to the enemy

   c. the time factor

   d. the volume of traffic

   e. the echelon of use

   f. the number of holders in a cryptonet

   g. the cryptoperiod

   h. the physical security conditions.

3. In making an assessment the security advisers will take into account the normal incidence of machine failures and operators' errors appropriate to the echelon and system in question.

~~TOP SECRET~~

ANNEX C to Appendix C to
LCS(53)/S/Report (Final Draft)

TITLE

U.K. CRYPTOGRAPHIC REQUIREMENTS PRO-FORMA

1. Title or Codename of equipment

2. Equipment to be used by:

   (a) Navy

   (b) Army

   (c) Air Force

   (d) NATO

   (e) Other

3. Level at which equipment is to be used

   (a) Navy

   (b) Army

   (c) Air Force

   (d) NATO

   (e) Misc.

4. (a) Type of Traffic to be passed on the equipment

   (1) Strategic

   (2) Tactical

   (b) Estimated proportion of higher classification

   (1) Top Secret

   (2) Secret and below

5. Volume per key

   (a) Desirable maximum

   (b) Acceptable minimum

6. Number of holders

~~TOP SECRET~~

~~TOP SECRET~~

7. Message length
   (a) Desirable minimum
   (b) Estimated average

8. Traffic peculiarities (Stereotyped; pro-forma, etc.)

9. Procedure
   (a) Disguised indicators
      (1) Acceptable
      (2) Unacceptable
   (b) Bisection
      (1) Acceptable
      (2) Unacceptable
   (c) Variable spacing
      (1) Acceptable
      (2) Unacceptable
   (d) Continuation procedure
      (1) Acceptable
      (2) Unacceptable

10. Category
   (a) Requirement for Publication
   (b) I/L Replies

11. Risk of physical compromise

12. Type of Operator
   (a) career
   (b) casual

13. Associated staff requirement

~~TOP SECRET~~

~~SECRET.~~

ANNEX C to LCS(53)/S/R6 (Final Draft).
dated 29th October, 1953.

TITLE

U.K. CRYPTOGRAPHIC REQUIREMENTS PRO-FORMA

1.	Title or Codename of equipment	
2.	Equipment to be used by:	
	(a) Navy	
	(b) Army	
	(c) Air Force	
	(d) NATO	
	(e) Other	
3.	Level at which equipment is to be used	
	(a) Navy	
	(b) Army	
	(c) Air Force	
	(d) NATO	
	(e) Misc.	
4.	(a) Type of Traffic to be passed on the equipment	
	(1) Strategic	
	(2) Tactical	
	(b) Estimated proportion of higher classification	
	(1) Top Secret	
	(2) Secret and below	
5.	Volume per key	
	(a) Desirable maximum	
	(b) Acceptable minimum	
6.	Number of holders	

~~SECRET.~~

7. Message length

   (a) Desirable minimum

   (b) Estimated average

8. Traffic peculiarities (Stereotyped; pro-forma, etc.)

9. Procedure

   (a) Disguised indicators

      (1) Acceptable

      (2) Unacceptable

   (b) Bisection

      (1) Acceptable

      (2) Unacceptable

   (c) Variable spacing

      (1) Acceptable

      (2) Unacceptable

   (d) Continuation procedure

      (a) Acceptable

      (b) Unacceptable

10. Category

   (a) Requirement for Publication

   (b) P/L Replies

11. Risk of physical compromise

12. Type of Operator

   (a) career

   (b) casual

13. Associated staff requirement

~~SECRET.~~