STANDARD FORM NO. 64

~~TOP SECRET~~ REF ID: A611615

Office Memorandum • UNITED STATES GOVERNMENT

TO AFSA-OOT DATE 17 August 1951

FROM Chief of Staff

SUBJECT Report of the U.K./U.S. Communications Security Conference held in London in July 1951

The inclosures are forwarded for your information and retention.

A. C. PETERSON
Colonel, Artillery
Acting Chief of Staff

Inclosures - 2 (bound together)

1. COPY NO. 13 of "Report to the British Chiefs of Staff and to the U.S. Chiefs of Staff of the U.K./U.S. Communications Security Conference Held in London in July, 1951"
2. COPY NO. 13 of Reports of the Working Parties (LCS/W1/R thru LCS/W12/R)

~~TOP SECRET~~

~~TOP SECRET~~

REPORT

of the

U.K./U.S. COMMUNICATIONS SECURITY CONFERENCE

HELD IN LONDON IN JULY, 1951

~~TOP SECRET~~ COPY NUMBER 13

~~TOP SECRET~~

JUL 31 1951

LCS/P/R.

Copy No: 13

REPORT

TO THE BRITISH CHIEFS OF STAFF AND TO THE U.S. CHIEFS OF STAFF OF THE U.K./U.S. COMMUNICATIONS SECURITY CONFERENCE HELD IN LONDON IN JULY, 1951.

1. In their endorsement of the report of the U.K./U.S. Communications Security Conference which was held in Washington in September 1950 the British and the U.S. Chiefs of Staff agreed:

> "That there be annual conferences on these subjects for the next four years to be held alternately in London and Washington, the first of these to be held in London in approximately nine months time".

2. In accordance with the above directive the 1951 Conference was opened in London on 6th July and closed on 31st July. The following items were discussed:-

On-line Cypher Machines.
Off-line Cypher Machines.
Replacement of the C.C.M. by BRUTUS.
Combat and Low Echelon Cryptosystems (including Authentication).
Merchant Ships Crypto systems.
Meteorological Cyphers other than Cifax.
Cifax.
Ciphony.
Cypher Key Generation.
Secure Wrapping of Cypher Material.
I.F.F.: Security aspects.

3. Reports of the various working parties which discussed the above listed subjects are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London.

4. The programme of 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 series of visits to establishments concerned in the research and development of communications security equipment.

5. The major recommendations of the Conference are that:-

(a) there be complete interchange of all projected equipments and technical information in the field of communications security so that the U.K. and the U.S. may carry out operational and security evaluations;

(b) there be visits of technicians as required and particularly whenever any equipment is ready for demonstration;

(c) in connection with the Brutus Cryptosystem:-

(i) there be no restriction on the level at which this system may be used, but, in accordance with the agreement between the British and the U.S. Chiefs of Staff, disclosure of the BRUTUS cryptosystem should be confined to the appropriate authorities in the U.S., U.K., Canada, Australia and New Zealand;

/(ii)

(ii) the use of this system be extended to Limited Combined Naval Low Echelon Communications;

(iii) A.F.S.A. and C.P.B. determine the operational procedure and the rules for the physical safeguarding of this system;

(d) the U.K./U.S. J.C.-E.Cs. be asked:

(i) to state what combined operational requirement exists for on-line cypher equipment;

(ii) to define the combined requirement for Air-Ground cryptosystems.

(iii) to define the combined requirement for teleprinter facilities to be incorporated in new off-line cypher machines, including such aspects as the teleprinter alphabet, keyboard and upper case facilities;

(iv) to state whether the "Personal Identity" recognition facility in I.F.F. equipment need be guarded by cyphering;

(e) the next Conference take place in three phases to be held consecutively in the following order, to ensure the closest liaison between the communications planning staffs, the security experts and the engineers:-

(i) Meeting between engineering and security experts of A.F.S.A. and C.P.B. to exchange detailed technical information and views.

(ii) Meeting between A.F.S.A. and C.P.B. to determine engineering possibilities and security standards.

(iii) Meeting between U.K. and U.S. communications planning staffs and representatives of A.F.S.A. and of C.P.B. to examine and define combined operational requirements and, where possible, to select equipments to meet them.

(f) the next Conference be held in Washington in April or May 1952.

6. The major recommendations in paragraph 5 above are submitted for the approval of the U.S. Chiefs of Staff and of the British Chiefs of Staff.

The detailed conclusions of the individual Working Parties, as endorsed by the Conference, are being submitted to the Director, Armed Forces Security Agency, and to the Cypher Policy Board for approval and further action.

Signed: Colonel S.P. Collins, U.S. Army.
Chairman of U.S. Delegation.

Signed: [redacted]
Chairman of the U.K. Delegation.

U.K./U.S. COMMUNICATIONS SECURITY CONFERENCE - 1951

Reports of the Working Parties

Reports of the Working Parties

~~TOP SECRET~~

LCS/W1/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

On-Line Cypher Machines.

Report of Working Party 1

as approved by the Executive Committee.

1. The Working Party reviewed the on-line cypher machines, available and projected, listed in paras. 3A - 3C below.

2. The Working Party discussed the possible operational requirements which the U.K. and U.S. Services have for such equipment and agreed that they appeared to fall into three categories:

A. Fixed Services (i.e. Synchronous exclusive point-to-point circuits)

B. Network Operation (including broadcasts)

C. Special Purposes (e.g. Hazardous operations, naval broadcasts, special missions, low echelon and combat purposes etc.)

3. The Working Party considered that it was not for them to determine whether there is a Combined requirement for equipment of this type. But if the UK/US JC-ECs or other competent authority decides that there is such a requirement, then it is recommended that the requirement be met by selection from the equipments listed below in accordance with the circumstances of the case.

A. Fixed Services.

(i) If the requirement arises now, the only equipments which could meet it are:-

(a) Apparatus 5 U.C.O. No. 1. Synchronous device using one time 5 unit tape. Size = One 6 foot x 19 inch rack per duplex terminal. Gives traffic flow security. Now in production.

(b) Circuit MERCURY. Synchronous 31 way permuting machine using a 6 + 4 double rotor maze and mechanical 5/31 converters for 5 unit code operation. Size = Two consoles and one 6 foot x 19 inch rack per duplex terminal. Now in production.

(ii) The following additional equipments should also be considered but will not be available for at least two years:-

(a) AFSAM 15. A synchronous modified version of AFSAM 9 using nine 36 point rotors as a 32 way permuting machine with built in 5/32 conversion for 5 unit code operation. Gives traffic flow security and automatic message numbering. Size = One 6 foot x 19 inch rack per duplex terminal.

/(b)

(b) ARTICHOKE A twin channel synchronous system using subtractor cypher key derived from an electronic key generator using multi-cold-cathode tubes. Gives traffic flow security. Size = One 6 foot x 19 inch rack per twin channel duplex terminal.

B. Network Operation

(i) If the requirement arises now, the only equipment which could meet it is:-

(a) AFSAM 9 A non-synchronous permuting machine using nine 36 point r tors and 5/32 conversion for 5 unit code operation. A light weight forward area equipment. Size = 16 x 12 x 6 inches, weight 27 pounds exclusive of teletype ancillary equipment.

(ii) The following additional equipment should also be considered but will not be available for at least three years:-

(a) ROLLICK MK II A non-synchronous device using subtractor cypher key derived from an electronic key generator using multi-cold-cathode tubes. Size = will not exceed one 4 foot 6 inch by 19 inch rack. (Note: ROLLICK Mk I is cryptographically unsuitable for network operation).

C. Special purposes

If a combined communication requirement arises at any time the following equipments, in addition to those listed above, might be available and should be considered:-

(i) AFSAM 309* A non-synchronous device using subtractor key derived from one time 5 unit tape. Consists of a basket containing a 5 unit tape reader to be inserted into the AFSAM 9. Size and weight of total equipment as for AFSAM 9.

(ii) AFSAM 44* A non-synchronous equipment which transmits "on line" and receives "off line". Tape operated only. Has two sensing heads, one for the message tape and one for the one-time key tape. Approximate weight 15 pounds. Size = 0.5 cubic feet.

(iii) AFSAM 45* A non-synchron us equipment designed for use with a printer or tape transmitter giving sequential 5 unit signals. Has one sensing head (for one time key tape) and selector mechanism. Approximate weight 20 pounds. Size = 0.5 cubic feet.

(iv) ROLLICK MK. I A non-synchronous device using subtractor cypher key derived from an electronic key generator using multi-cold-cathode tubes. Size = one 4 foot 6 inch x 19 inch rack. Now in production.

(v) ROCKEX A non-synchronous device using subtractor key derived from one-time 5 unit tape. Provides an all-letter

* These equipments will interwork.

/crypt.

~~TOP SECRET~~

crypt. Transmits "on-line" and receives "off-line". Has two sensing heads, one for the message tape and one for the key tape. Size = (including its own table) 20 inches x 22 inches x 38 inches (high); total weight about 200 lbs; exclusive of ancillary equipment. Now in production.

4. The Working Party further recommended that all projected equipments and detailed information about them should be exchanged at the first opportunity so that the U.K. and the U.S. could carry out operational and security evaluations.

10th July, 1951.

~~TOP SECRET~~

LCS/W2/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

Off-Line Cypher Machines.

Report of Working Party 2

as approved by the Executive Committee.

1. The Working Party devoted a full day to a review of off-line cypher machines which are in various stages of research, development and production but which are not in current use.

2. The following machines came under review, those marked with an asterisk being demonstrated:-

		Relevant Papers	BRUSA C/S
	U.K.		
1.*	PORTEX (D.U.P.1)	Description	508
		Security assessment	509
		Security assessment	12
2.*	SINGLET	Description of bigramming device	512
3.	PENDRAGON		
4.*	Permuting M.209	Description	504
		Security assessment	513
5.	Electronic Cypher machine	Description	515
6.	do.	Description	516
7.*	ROCKEX: Security modifications	Description	517
	U.S.		
8.*	AFSAM 7	Description and security assessment	1
		Description and security assessment	13
		Security assessment	536
9.	AFSAM 36 (M.C.M.)	Description and security assessment	3
		Description and security assessment	15
10.	AFSAM 47 (P.C.M.)	Description and security assessment	16
11.*	DEM 17	Description	18

~~TOP SECRET~~

			BRUSA C/S
12.*	DEM 21	Description and security assessment	19
13.	Alphabet Generator machine	Description	40
	Others		
14.	M.209: French modifications	Description and security assessment	518

3. The Working Party wish to record that there was the most free discussion of all aspects of these machines, that the resultant interchange of views was of great value to the representatives of both countries and that no important points of disagreement came to light.

4. The Working Party further recommended that all projected equipments and detailed information about them should be exchanged at the first opportunity so that the U.K. and the U.S. could carry out operational and security evaluations.

9th July, 1951.

~~TOP SECRET~~

LCS/W3/R. Approved. Copy No: 13

U.K./U.S. COMMUNICATIONS SECURITY CONFERENCE 1951.

Replacement of the C.C.M. by BRUTUS and Improvements to the Existing C.C.M.

Report of Working Party 3
as approved by the Executive Committee.

A. Replacement of the C.C.M. by BRUTUS.

1. The BRUTUS MAZE.

The Working Party considered the security of the maze for the BRUTUS cryptographic system and made the following recommendations:-

(a) that the ROTOR MOVEMENT should be such that the rotors in positions two and six should step in opposite directions to the rest of the rotors: these latter step in the direction of the present CCM (AJAX);

(b) that the ROTOR STEPPING ORDER should be as follows:-

(i) Rotor 4 steps with each encypherment.
(ii) Rotor 6 steps if rotor 4 is in a notched position.
(iii) Rotor 2 steps if both rotors 4 and 6 are in notched positions.
(iv) Rotor 7 steps if rotor 2 is in a notched position.
(v) Rotor 1 steps if rotor 7 is in a notched position.
(vi) Rotor 5 steps if rotor 1 is in a notched position.
(vii) Rotor 3 steps if rotor 5 is in a notched position.

(c) that REMOVABLE CAM CONTOURS as recommended by the 1950 U.K./U.S. Communications Security Conference for use with the existing C.C.M. should be adopted for BRUTUS and that the U.K. and the U.S. technicians should exchange technical information and prototypes in order that the most suitable design should be adopted for common use by all Services. As, during operation, only one side of a rotor is used to effect the stepping motion each set of rotors should be provided with a set of removable cam contours with identity numbers but with no alphabet and a set of alphabet rings without contours. In use, therefore, each rotor would be fitted with one removable cam contour and one alphabet ring;

/(d)

(d) that the number of notches in the NOTCH PATTERN on any removable cam contour should not be other than 7, 9, 11, 15, 17 or 19. The questions of consecutive notch patterns, the possible provision of special high incidence notch cam contours for the centre rotor and the reversibility of the notch ring should be the subject of further study and an exchange of views between the U.S. and U.K. cryptographic security agencies;

(e) that a SET OF ROTORS should consist of ten rotors;

(f) that the WIRING of each rotor in a set should be different and that the wiring of each individual rotor should contain 18 distinct intervals (i.e. different wire lengths), the remaining intervals falling where they may.

In considering the rotors for the BRUTUS cryptosystem the Working Party took note of the fact that for the C.C.M. the U.K. and the U.S. Services were committed to rotors of different sizes and recommended that there should be no attempt at standardisation for existing equipments.

2. Other BRUTUS Security Factors.

The Working Party considered the other security factors relative to the BRUTUS cryptographic system.

(a) Compilation of Key Lists.

(i) The Working Party took note of a U.S. proposal to produce an equipment to speed up compilation of key lists and recommended that the U.K. cryptographic agency be provided with details as they become available.

(ii) The Working Party took note of the U.K. method of printing key lists with the first day of the period at the bottom of the sheet to facilitate early destruction of obsolete keys in hazardous areas and recommended that the application of this method to BRUTUS key lists should be examined.

(b) Indicator and Operating Procedures.

The Working Party took note that the prime user requirement was for the simplest procedure compatible with security. Subject to this general observation the Working Party recommended that the Indicator Procedure and the Operating Procedure for the BRUTUS cryptosystem should be the subject of further study and an exchange of views between the U.K. and the U.S. cryptographic security agencies.

/3.

3. Restriction on the Operational Use of BRUTUS.

The Working Party recommended that there should be no restriction on the level at which the BRUTUS cryptosystem could be used but that in accordance with the agreement between the U.S. and the U.K. Chiefs of Staff disclosure of the BRUTUS cryptosystem should be confined to the appropriate authorities in the U.S.A., U.K., Canada, Australia and New Zealand.

4. Requirement for Teleprinter Facilities in machines embodying BRUTUS.

(a) The Working Party considered the following draft recommendation made by representatives of the B.J.C.E.B. and the U.S. J.C.-E.C. at their joint meeting held in London in June 1951:-

"The B.J.C.E.B. and the U.S. J.C.-E.C. after considerable discussion agreed that it was desirable for Combined off-line cypher equipments, which would be designed in the future, to handle the full range of the Combined teleprinter alphabet and to operate from a standard teleprinter keyboard".

(b) The Working Party noted that the B.J.C.E.B. and the U.S. J.C.-E.C. were, at the time, discussing only off-line equipments. Had on-line equipments been under discussion the same recommendations would, no doubt, have been made.

(c) After considerable discussion the Working Party concluded that the present variation in designs of the keyboard on existing U.K. and U.S. off-line cypher equipments arose from a fundamental difference in message writing procedure adopted by the respective Service Staffs. Until this difference in staff practice was resolved it would be extremely difficult to resolve the cryptographic problem. Bearing in mind that the new series of A.C.P.'s might help to resolve the staff differences, the Working Party recommended that the provision of full teleprinter keyboard facilities on future off-line cypher machines should be the subject of further study and exchange of views and that this subject should be raised again at the next U.K./U.S. Communications Security Conference.

B. The Existing C.C.M.

5. Improvements to the Existing C.C.M.

(a) The Working Party reviewed the steps taken to improve the security of the existing C.C.M. in accordance with the recommendations of the 1950 U.K./U.S. Communications Security Conference and noted:-

(i) that additional rotors to increase the size of all sets used for U.K./U.S. traffic from 10 to 20 rotors per set were in course of production and that all U.K./U.S. C.C.M. cryptosystems should be based on sets of 20 rotors by 1st January, 1953;

/(11)

~~TOP SECRET~~

(ii) that the U.K. and the U.S. had solved the problem of fitting removable cam contours to their respective rotors but no exchange of such rotors for trials had yet taken place. As soon as this exchange shall have taken place and the final design had been agreed, production will be initiated and the system introduced as soon as possible;

(iii) that a new disguised indicator procedure had been worked out by the U.K. and U.S. cryptographic security agencies and this procedure was awaiting ratification by the U.K.-U.S. J.C.-E.C's with a view to its introduction on a Combined basis as soon as possible;

(b) The Working Party considered the operating procedures for C.C.M. at present in force and recommended:-

(i) that VARIABLE SPACING should be applied to all messages. The slight difference between existing U.K. and U.S. procedure has been reconciled and steps will be taken to introduce the agreed procedure as soon as possible;

(ii) the BISECTION PROCEDURE should be applied to all messages and in long messages should be applied once in each cryptographic part;

(iii) that SHORT MESSAGES should not be padded;

(iv) that the use of SIMPLEX SETTINGS should be considered with the present C.C.M. (AJAX) whenever overall long-term security is required at the higher levels irrespective of whether the other security refinements recommended had been introduced and, with this end in view, that a study should be made of the problems involved in the compilation, production and operational use of Simplex Settings with the C.C.M.;

(v) that C.C.M. PROCEDURE for use on NATO cryptonets should be the same as on combined nets.

11th July, 1951.

~~TOP SECRET~~

LCS/W4/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

Combat and Low Echelon Cryptosystems (including Authentication).

Report of Working Party 4

as approved by the Executive Committee.

1. The Working Party took as the basis of their deliberations Annex 'F' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs.

Combat Systems

2. (a) Navy

IT WAS AGREED that since the UK/US JC-ECs. had not reached agreement as to whether a Combined major war vessels tactical cryptosystem was required, no progress on this item could be made.

(b) Army

(i) Air Support Control Codes.

A. IT WAS AGREED:-

1. that the requirement under this item would eventually be met by the provision of suitable ciphony equipment;

2. that pending the provision of such equipment it would be necessary to use special purpose codes.

B. IT WAS NOTED:-

that the British Army were considering the use of a short vocabulary code recyphered by one time pad (ASREX) for this purpose.

C. IT WAS RECOMMENDED:-

that ASREX should be studied with a view to possible combined use.

(ii) Map Reference Codes.

A. IT WAS AGREED:-

1. that the requirement under this item would eventually be met by the provision of suitable ciphony equipment;

2. that pending the provision of such equipment it would be necessary to use special purpose codes.

/B.

B. IT WAS NOTED:-

1. that the U.S. Army relied on locally produced codes for this purpose.

2. that the British Army used UNICODE but that the security of the system was low.

3. that the British Army was considering the following systems for this purpose:-

MAPFRAX
Double MAPLAY

C. IT WAS RECOMMENDED:-

that MAPFRAX and Double MAPLAY should be studied with a view to possible Combined use.

(iii) Status Reporting Codes
Forward Echelon Voice Codes

A. IT WAS NOTED:-

that the UK/US JC-ECs. considered that there was no requirement for Combined agreement on these systems.

(c) Air Force (Ground-Ground)

(i) Aircraft Movements Code

A. IT WAS AGREED:-

that the requirement under this item might be met by the provision of a suitable light weight off-line machine crypto-system.

B. IT WAS NOTED:-

that a special purpose code for this purpose was currently under discussion by the UK/US JC-ECs.

(ii) Friendly Aircraft Approach Code
Ground Radar Reporting Codes

A. IT WAS NOTED:-

that the UK/US JC-ECs. considered that there was no requirement for Combined agreement on these systems.

(d) Air-Ground

(i) Maritime and U-boat Warfare
Bomber and Supply/Troop Dropping Operations

A. IT WAS AGREED:-

1. that the requirement under this item might be met by the provision of a suitable light weight off-line machine cryptosystem.

~~TOP SECRET~~

2. that pending the provision of such a system it would be necessary to use vocabulary codes for this purpose.

B. IT WAS NOTED:-

that the provision of such vocabulary codes was currently under discussion by the UK/US JC-ECs.

(ii) Meteorological

A. IT WAS AGREED:-

that consideration of this item should be referred to Working Party No. 6.

(e) Amphibious Operations

A. IT WAS AGREED:-

1. that the requirement under this item might be met by the provision of a suitable light weight off-line machine crypto-system.

2. that pending the provision of such a system it would be necessary to use a vocabulary code for this purpose.

B. IT WAS NOTED:-

that the UK/US JC-ECs. had recently agreed that such a Combined code should be provided and that AFSA and GCHQ were currently engaged in its compilation and production.

(f) Authentication

A. IT WAS NOTED:-

1. that authentication publications were currently under discussion by the UK/US JC-ECs.

2. that AFSA had under development two authentication devices for challenge and reply use on limited communication nets:-

ASAD 2 (x - 1)
ASAD 2 (x - 2)

B. IT WAS RECOMMENDED:-

that further consideration should be given to ASAD 2 (x - 1) and ASAD 2 (x - 2) with a view to their possible adoption for Combined use.

/Low Echelon

~~TOP SECRET~~

~~TOP SECRET~~

Low Echelon and Combat Systems in General

3. The three main Combined low echelon and combat requirements stated by the J.C.-E.C. are:-

(a) Naval low echelon communications

(b) Air-Ground Communications

(c) Amphibious Communications

4. The Working Party considered the hand cryptosystems which will be available within the immediate future. It was agreed that the following will be available:-

Strip
LINEX
PLAYFEX
Vocabulary Codes

5. The Working Party also considered the machine systems likely to be available for intermediate and long term solution of the requirements in paragraph 3 above. These machine systems are:-

U.K.	U.S.
PORTEX	M.C.M. AFSAM 7 AFSAM 47 DEM 17

It was noted that:-

(a) delivery of the first 50 models of PORTEX for field trials was about to begin. The date on which quantity production could begin depended on the length and outcome of field trials but tools existed for the manufacture of a limited number of machines should they be required in emergency prior to the completion of field trials. By the end of 1953 production could be built up to 100 machines a week;

(b) arrangements for the production of MCM were well in hand. Providing the equipment proved satisfactory delivery would start within a year and it was expected that 2,000 machines would be available within two years. Thereafter there would be a production potential of 30-40,000 machines a year;

(c) although Service test trials were not yet complete, tooling for production of AFSAM 7 had begun. It was expected that by 1952 the production capacity would be 5,000 machines a year;

(d) arrangements for the production of AFSAM 47 would follow. No dates or production capacity could yet be definitely stated, but a production rate of 500 a month could be attained by 1953;

/(e)

(e) a first model of DEM 17 was demonstrated to the Working Party and development of an improved model was being pursued as rapidly as possible.

6. For security reasons, and in the light of present cryptographic techniques, it was agreed that, wherever operational circumstances permitted, more than one cryptosystem should be used for Combined literal cypher purposes.

7. Naval Low Echelon Communications.

(a) Short term solution.

It was agreed that only hand systems are available for limited Combined naval use, and that the choice lies between the following two systems:-

Strip
PLAYFEX

It is recommended that as soon as possible U.K. and U.S. should carry out operational and security evaluations of the above systems respectively, with a view to reaching agreement on which system should be used.

(b) Intermediate and long term solutions.

It was agreed that limited Combined naval communications should be treated as an exception to the principle recommended in paragraph 6 above and that the Brutus cryptosystem should be used both for low echelon and high echelon communications. It was noted that after trials of AFSAM 7 and AFSAM 47 the U.S.N. are likely to adopt one of those equipments for intra-Naval use. The Working Party therefore recommended that as a matter of urgency, the U.K. should develop a parallel machine employing the BRUTUS technique.

8. Air-Ground Communications.

Certain aspects of air-ground communications have already been covered in paragraph 2(d) above. The Working Party considered that the requirement for combined cryptosystems for air-ground communications requires clarification. Where a machine requirement exists, it could probably be met by one of the equipments described in paragraph 5 above.

9. Amphibious Communications.

(a) Short term solution.

This is covered in paragraph 2(e) B above.

(b) Intermediate and long term solution

It was agreed:-

(i) that there is probably a requirement for a mechanically operated off-line cypher machine and for an electrically operated analogue of such machine.

(ii) that the M.209 principle appeared less suitable than a permuting maze from the security angle, and also owing to the difficulty of providing sufficiently speedy operation in an electrical analogue.

(iii) that it is not yet possible to make detailed recommendations on what machine should be used.

10. Exchange of Equipments.

It was recommended that all projected equipments and detailed information about them should be exchanged at the first opportunity so that the U.K. and U.S. could carry out operational and security evaluations.

26th July, 1951.

~~TOP SECRET~~

LCS/W5/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

Merchant Ships' Cryptosystems.

Report of Working Party 5

as approved by the Executive Committee.

1. The Working Party took as the basis of their deliberations Annex 'C' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs.

The Present Situation.

2. The Working Party reviewed the present situation.

IT WAS NOTED:-

(a) that a quantity of merchant ship crypto-material left over from World War II was available for issue in the event of war in the immediate future.

(b) that arrangements for the production of the Merchant Ship Cipher Device (ACP 212) and associated key material, which would replace World War II systems, had been agreed between AFSA and GCHQ. Production would begin immediately. The Device and associated key material should be available for issue in the Spring of 1952.

Replacement of the Merchant Ship Cipher Device (ACP 212) by a Machine.

3. IT WAS AGREED that the following proposed amendments to Annex 'C' of the paper C/SC 55 should be forwarded to the UK/US JC-ECs. for consideration:-

(a) Amend paragraph 1 to read:-

"1. Combined communications are required. It is essential that Canadian, U.K., U.S. and allied naval authorities and warships should be able to communicate with any Canadian, U.K., U.S. or allied merchant ship and with any neutral merchant ship trading in the allied interest."

(b) Amend paragraph 7 to read:-

"7. Cypher Machine - Drive. Manual or power drive will be acceptable. If manual drive is provided a power driven cryptographic analogue should also be provided."

/4.

~~TOP SECRET~~

4. The Working Party reviewed the machine crypto-systems available and projected. These were:-

PORTEX
MCM
AFSAM 7
AFSAM 47
DEM 17
Permuting M.209
French M.209
Any new machine which may be developed for low echelon use.

IT WAS AGREED:-

(a) that in selecting a suitable cypher machine for merchant ship communications it was necessary to pay particular attention to the aspects of cost and simplicity.

(b) that for these reasons provision of a merchant ship cypher machine was a separate problem not necessarily related to the problem of providing a low echelon cypher machine for Service use. However it would obviously be a great advantage if the same basic machine could serve both purposes.

(c) that it was not possible at this stage to recommend a particular machine for merchant ship use since further development and experience of the various machines listed above was first required.

(d) that failure to recommend a particular machine at this time would in no way delay solution to the problem since development of all possible machines was progressing at a rate as rapid as available funds permitted.

13th July, 1951.

TOP SECRET

LCS/W6/R. Approved. Copy No: 13

UK/US Communications Security Conference, 1951.

Meteorological Cyphers other than Cifax.

Report of Working Party 6 as approved by the Executive Committee

1. The Working Party took as the basis of their deliberations Annex 'G' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs.

2. IT WAS AGREED that the following proposed amendment to Annex 'G' of the paper C/SC 55 should be forwarded to the UK/US JC-ECs. for consideration:-

(a) Amend paragraph 2(c) to read:-

"(c) Manual (preferably one-time)".

Examination of the Combined Operational Requirements.

On-line Equipment

3. The Working Party reviewed the on-line crypto-systems available and projected. These were:-

AFSAM 15 Apparatus 5 U.C.O. No. 1 Circuit MERCURY ARTICHOKE	Synchronous
AFSAM 2 - 1 AFSAM 9 ROLLICK	Non - Synchronous
Conventional one time tape systems	

IT WAS AGREED:-

(a) that it was not possible at this time to select any particular equipment for Combined use. Selection from the above systems could best be made when the requirement for on-line equipment arose and depending on circumstances ruling at the time.

Off-line Equipment.

4. (a) General Dissemination of Weather Information.

A. IT WAS AGREED:-

1. that for UK/US use the present CCM modified for weather encypherment (that is using a weather switch such as AFSAM 100) could be used for this purpose as soon as the necessary modification kits, special rotors and key lists could be made available;

2. that when the BRUTUS system replaced the present CCM for UK/US use it too could be used for weather encypherment provided special rotors and key lists were used.

/(b)

TOP SECRET

(b) Weather Reporting Posts and Met. Reconnaissance Flights.

A. IT WAS NOTED:-

1. that in the immediate future the UK Services intended to use one time pads;

2. that AFSA had under development a digital form of the DEM 21 (M.209 modified for one time tape operation) and that this equipment might prove suitable for the transmission of reports from posts and aircraft to collecting centres;

3. that the U.K. had under consideration a modification to PORTEX to make it suitable for the encypherment of met. data.

B. IT WAS AGREED:-

1. that the one time pad was the only system immediately available;

2. that further consideration should be given to a digital form of the DEM 21 and PORTEX with a view to their possible adoption for this purpose.

(c) Air-Ground.

A. IT WAS NOTED:-

1. that for the transmission of weather information to aircraft in flight the Royal Air Force used the UCO system;

2. that AFSA had under development two devices for this purpose:-

ASAD 1 (X - 2)
ASAD 1 (X - 3)

B. IT WAS AGREED:-

1. that UCO was the only system immediately available, and should be considered for Combined use. It was used successfully during World War II by both the Royal and U.S. Air Forces;

2. that further consideration should be given to ASAD 1 (X-2) and ASAD 1 (X-3) with a view to their possible adoption for Combined use;

3. that further development of ASAD 1 (X-3) was highly desirable in any case since it was also likely to be valuable in other fields, e.g. "Status" Reporting Codes;

4. that for the transmission of landing weather information ciphony equipment is recommended as the long term solution.

The Implications of NATO on the Foregoing Requirements.

On-line Equipment.

5. IT WAS AGREED:-

that should it be decided to issue on-line equipment to NATO powers, conventional one-time tape systems were to be preferred. The use of these would protect UK/US cryptographic techniques and the equipment was the most likely to be available.

/6.

Off-line Equipment.

6. (a) General Dissemination of Weather Information.

A. IT WAS AGREED:-

1. that to protect UK/US cryptographic techniques the only system which could be considered for this purpose was the present CCM modified for weather encypherment (that is using a weather switch such as AFSAM 100);

2. that owing to the small number of CCM machines available it was unlikely that this equipment could be provided in sufficient quantity for NATO met. purposes for at least two years;

3. that no other system was available and therefore in the interim period it would be necessary for each NATO power to use its own national met. systems with ad hoc arrangements for the dissemination of information to other powers.

(b) Weather Reporting Posts and Met. Reconnaissance Flights.

A. IT WAS AGREED:-

that provision of suitable systems for these purposes should be the individual responsibility of each NATO power.

(c) Air-Ground.

A. IT WAS AGREED:-

1. that it was highly desirable that a common system be held by all NATO powers for the transmission of weather information to aircraft in flight;

2. that UCO was the only UK or US system immediately available for this purpose.

Exchange of Equipment.

7. IT WAS RECOMMENDED that all projected equipments and detailed information about them should be exchanged at the first opportunity so that the U.K. and the U.S. could carry out operational and security evaluations.

20th July, 1951.

~~TOP SECRET~~

COPY NO: 13

LCS/W7/R Approved

UK/US Communications Security Conference, 1951

C I F A X

Report by Working Party 7

as approved by the Executive Committee.

1. The Working Party discussed the following equipments :-

U.K.	U.S.
METFAX	AN/UXC 2
	ASAX 3

2. The Working Party took note of Annex 'D' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs. They considered that joint operational requirements were at present too undecided for any combined agreement to be reached.

3. The Working Party agreed that, should a requirement arise during the next two years for an equipment for combined use, selection could only be made from the following equipments which might be available in limited quantity :

AFSAY 806 (referred to in Report of Working Party 8)

AN/UXC 2

METFAX

4. It was recommended that all projected equipments and detailed information about them should be exchanged at the first opportunity so that the U.K. and the U.S. could carry out operational and security evaluations.

26th July, 1951.

~~TOP SECRET~~

~~TOP SECRET~~

LCS/W8/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

C I P H O N Y

Report of Working Party 8

as approved by the Executive Committee.

1. The Working Party reviewed the following U.K. and U.S. Ciphony equipments and projects:-

U.K.	U.S.
BANGLE	AFSAY 806
HALLMARK I	ASAY 8
HALLMARK II	ASAY 4
PICKWICK	ASAY 5
D.70	AN/TRC 25-ASAY 7
WHISPER	Vocoder basic research
SORCERER	
TRUMPETER	

2. The Working Party had detailed technical discussions on all the items listed above, including demonstrations where practicable.

3. The Working Party took note of Annex 'E' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs. but concluded that, for the present, no recommendations could be made about the selection of equipment to meet combined requirements as now stated.

4. The Working Party took note:-

(a) that the U.S. Air Force considered that secure air/ground and air/air communications were matters of the highest priority, and had therefore defined to A.F.S.A. the military characteristics of a ciphony system which A.F.S.A. was already committed to develop.

(b) that existing U.S. U.H.F. and V.H.F. air/ground and air/air radio sets could be used to transmit and receive ciphony of the general type requiring binary transmission at a rate of about 24,000 bauds per second with virtually no modification to the sets concerned.

(c) that the ciphony equipment AFSAY 806 could encypher black/white facsimile or 3 channel teletype as alternatives to speech. Furthermore that Bangle could be adapted to encypher half tone facsimile pictures.

/5.

5. The Working Party suggested that the U.K. and U.S. Services, in formulating their ciphony requirements, might find it helpful to make operational trials of pulse code modulation as a communication technique without security equipment. The attachment of a security device to the P.C.M. equipment would not alter the communications characteristics of the latter. These trials would enable the Services to assess the inherent operational complications arising from the use of encyphered speech.

6. The Working Party concluded that no tactical ciphony system in the 2-30 mcs. frequency range suitable for either shipborne or vehicular use would be available in the near future.

7. The Working Party recommended that all projected ciphony equipments and detailed information about them should be exchanged at the first opportunity so that U.K. and U.S. could carry out operational and security evaluations.

25th July, 1951.

~~TOP SECRET~~

LCS/W9/R Approved

COPY NO: 13

UK/US Communications Security Conference 1951.

CYPHER KEY GENERATION.

Report of Working Party 9.

as approved by the Executive Committee.

1. The Working Party reviewed the following equipments and projects for the generation, production and checking of cypher key:-

U.K.	U.S.
TRIMMER	ASAF 44 (high speed recorder)
ROCKEX Key Generating Equipment	AFSAL 5116
5 U.C.O. Key Generating Equipment	One time Key Generator for AFSAY 806
Key Tape Checker	

2. The Working Party took note that there was no combined operational requirement for key tape generating equipment. The 5 unit Key tapes used by both the U.K. and the U.S. are interchangeable and the equipment of either nation could therefore be used according to circumstances. It was agreed that the combined standard of randomness detailed in Appendix A should be accepted and that the situation should be reviewed at all future conferences as a regular item of the agenda.

3. The Working Party recommended the following exchange of information:-

(a) The U.S. to supply:-

(i) Outline description together with photographs of AFSAF 44.

(ii) A model of the 900 operations per minute perforator.

(iii) The manufacturing specification for paper tapes together with samples of the 5-unit and 7-unit sizes, including the description of the ageing test with experience of wear on machines.

(iv) Further information on how the number of breaks had been limited in the recently supplied ROCKEX tapes.

(b) The U.K. to supply:-

(i) Full details of the high speed Checker.

(ii) Details of "The Timms Counter".

(iii) A model of the 100 unit perforator (three headed punch).

26th July, 1951.

~~TOP SECRET~~

~~TOP SECRET~~

APPENDIX A

Randomness in key is intended to prevent discrimination between key and the random expectation in the type of Key material generated. This is a quantitative effect and practical considerations place a limit on the randomness.

The following limits have been agreed:-

(i) Keys showing a deviation of 2 sigma or less from random in all counts are acceptable.

(ii) Any Key showing a deviation in any count of 4 sigma or more from random expectancy is unacceptable.

(iii) No Key showing a deviation in any count of between 2 sigma and 4 sigma from random expectancy may be used without further examination.

(Note that these criteria may be stated either in terms of sigma as above or in terms of the appropriate probabilities.)

2. Counts to be made must depend on the actual method of generation. However, the following counts based on stretches of at least 10,000 consecutive units of Key are common to all methods and will apply to all types of Key tapes.

(i) Frequency count of single units of Key.

(ii) " " " consecutive pairs of units of Key (for binary material the mod 2 sum of consecutive pairs).

(iii) Suitable multi-unit counts to ensure correct operation of the generating and recording equipment (for binary material runs of 15 consecutive delta dots and delta crosses are counted).

3. For multi-level key these counts will be made for each level independently and for the units of Key considered as one stream in the order of emission from the generator.

~~TOP SECRET~~

Copy No: 13

LCS/W10/R Approved

UK/US Communications Security Conference 1951

Secure Wrapping of Cypher Material

Report of Working Party 10

as approved by the Executive Committee

1. The Working Party reviewed the systems of protecting cryptographic documents demonstrated by the British members as follows:-

Security wrapped pads

Pads with sealed edges

Welded plastic envelopes

2. The Working Party took note of Annex 'B' of the paper C/SC 55, dated 21st June, 1951, prepared by the UK/US JC-ECs. and noted that none of the projected schemes could be expected to give protection under circumstances other than those in which an Agent had only limited time and facilities at his disposal.

3. The Working Party recommended that samples of the systems demonstrated should be supplied to the U.S. for study and comment.

4. The Working Party recommended that there should be a continuing exchange of ideas and techniques.

27th July, 1951.

~~TOP SECRET~~

~~TOP SECRET~~

COPY NO: 12

LCS/W11/R Approved

UK/US Communications Security Conference, 1951

I.F.F.: Security Aspects

Report by Working Party 11

as approved by the Executive Committee

1. The Working Party discussed in considerable detail the various U.K. and U.S. proposals for an I.F.F. Security System.

2. The Working Party concluded that the techniques of neither nation had yet reached a sufficiently advanced stage for it to be possible to recommend equipment for Combined use but they agreed that future development should take into consideration the following factors:-

(a) That the code system should be inviolable to cryptanalytic attack by cataloguing challenges and replies. To this end the total possible challenges and replies on any one setting should probably exceed 10^6.

(b) That an automatic zeroising system operating whenever a plane lands or crashes is desirable to reduce the risk of physical compromise of daily settings of the coding device.

3. The Working Party recommended that the UK/US JC-ECs be asked to state whether the "Personal Identity" recognition facility need be guarded by cyphering or not.

4. The Working Party considered that the exchange of views had been most valuable and they further recommended that both A.F.S.A. and C.P.B. should maintain close contact with those responsible for the development of new I.F.F. security equipment in the U.S. and U.K. respectively, so that, when combined equipment eventually came to be considered, the equipment developed in both countries would be cryptographically sound.

20th July, 1951.

~~TOP SECRET~~

~~TOP SECRET~~

Copy No: 13

JCS/W12/R Approved.

Provision of Upper Case Facilities on Off-Line.

Cypher Machines for Combined U.K./U.S. Use.

Report of Working Party No. 12 as approved by the Executive Committee.

1. The Working Party met to consider the provision of upper case facilities on Off-Line Cypher machines for Combined Use.

(a) for general usage

(b) for weather traffic

Only machines employing the CCM(AJAX) or the BRUTUS cryptographic systems were considered.

2. As a basis for discussion the Working Party accepted the following principles:-

(a) that it was not yet possible to agree on the design for a Combined off-line machine which would handle the full range of the Combined teleprinter alphabet and operate from a standard teleprinter keyboard (see report of Working Party No.3 paragraph 4);

(b) that the provision of limited upper case facilities on Combined off-line cypher machines was preferable to providing no upper case facilities at all.

3. The Working Party considered the keyboard layouts of teleprinters, teletypewriters and off-line cypher machines already in production or about to be produced (see comparative table attached) and reached the following conclusions:-

(a) Provision of Upper Case Facilities for CCM (AJAX).

(i) General Usage.

Except for the numerals and five punctuation marks the upper case characters on the Typex machine are non-standard. In addition, the Typex uses the Z circuit for FIGURE SHIFT; U.S. machines use the new J circuit. There is, therefore, no possibility of providing a general purpose Combined machine cryptosystem using upper case characters until the Typex is replaced in the U.K. Services.

(ii) Weather Traffic.

The provision of upper case facilities for weather traffic in the CCM(AJAX) cryptosystem would require further consideration. Proposals to meet the requirement should be exchanged by A.F.S.A. and C.P.B. and, if possible, a decision should be reached before the next Conference.

/(b)

~~TOP SECRET~~

~~TOP SECRET~~

(b) Provision of Limited Upper Case Facilities on machines employing the BRUTUS principle.

(i) The direct encryption of ten upper case characters (the numerals 0-9) can be achieved by adopting the following basic wiring scheme on AFSAM 47 (PCM), AFSAM 7, SINGLET and such other U.K. or U.S. equipments as may be designed for BRUTUS working:-

X	Key to be taken through the X circuit								
Z	"	"	"	"	"	"	X	"	
Space	"	"	"	"	"	"	Z	"	
Y	"	"	"	"	"	"	Y	"	
J	"	"	"	"	"	"	Y	"	
Figures	"	"	"	"	"	"	J	"	
Letters	"	"	"	"	"	"	Upper case V circuit		
Lower case V	"	"	"	"	"	"	V circuit		

(ii) If AFSAM 47(PCM) and SINGLET only were to work together the following additional eight upper case characters could be encrypted - ( ) / : ? , ..

(iii) In the present CCM(AJAX) cryptosystem the letter Z decrypts as X. In this scheme, in addition, the letter J will decrypt as Y.

(iv) For U.S. machines, the full scheme is incorporated in the present design for AFSAM 47(PCM) and the limited (numerals only) scheme is incorporated in the design for AFSAM 7.

(v) For U.K. machines:

(1) It will not be possible to introduce the schemes in paras. 3(b)(i) and 3(b)(ii) above until the U.K. Services cease to use Typex with a BRUTUS adaptor.

(2) For Combined working the bigramming feature on SINGLET/PENDRAGON will not be used.

(vi) In order to limit the differences between the above method for securing limited upper case facilities and the bigramming method of securing full teleprinter facilities the U.K. Services will use the following wiring system on SINGLET/PENDRAGON.

FIGURES KEY	to be taken through			J	circuit	
BIGRAM KEY	"	"	"	"	K	"
LETTERS KEY	"	"	"	"	V	"

4. The Working Party made the following recommendations:-

(a) that it be noted that until the U.K. and the U.S. Services cease to use their current equipments with the CCM(AJAX) or BRUTUS adaptors modification to provide upper case facilities other than for weather traffic will be extremely difficult.

(b) that until a Combined Communication Policy is agreed all cypher machines designed for UK/US use in the future should include at least the limited upper case facilities as set out in para. 3(b)(i) above.

(c) that should the CCM(AJAX) be used for weather traffic the particular cryptosystem in question must handle weather traffic exclusively.

Telegraph and Cypher Machines.
Comparative Table of Upper Case Characters.

Upper Case Equivalent.

Lower Case Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Remarks
Teletype	-	'	:	ø	3	!	&	STOP	8	'	(	)	.	,	9	ø	1	4	BELL	5	7	;	2	/	6	"	The numerals 0-9 and - ? : ( ) . , / are common upper case characters
Teleprinter	-	?	:	WHO R U	3	%	@	£	8	BELL	(	)	.	,	9	ø	1	4	'	5	7	=	2	/	6	+	
COMBINED TELEPRINTER ALPHABET	-				3				8		(	)	.		9	ø	1	4		5	7		2	/	6		Authorised by ACP 126
Typex	-	'	V	Z	3	%	X	£	8		(	)	.	,	9	ø	1	4	/	5	7	↓	2	SPACE	6	↑	Z = figures circuit. X = space circuit. V = letters circuit.
CSP 1700																											No upper case.
AFSAM 7	A	B	C	D	3	F	G	H	8	↑	K	L	M	N	9	ø	1	4	S	5	7	↓	2	X	6	SPACE	
AFSAM 47 (PCM)	-	?	:	D	3	F	G	H	8	J	(	)	.	,	9	ø	1	4	S	5	7	↓	2	/	6	SPACE	Current Production model J Key used for figures circuit.
SINGLET	-	?	:		3	%	@	£	8	BIGRAM	(	)	.	,	9	ø	1	4	'	5	7	=	2	/	6	+	To give full teleprinter facilities Z, B, K, J, LF, CR are bigrammed. Bigram key used J circuit.
CSP 1700 with AFSAM 100 (Weather Switch)	A	B	C	D	3	F	G	H	8	J	K	L	M	N	9	ø	1	4	S	5	7	V	2	X	6	SPACE	