844

~~TOP SECRET~~

Copy No 1.

U.S

OK with changes

LCS(53)/OR/R3 (Final Draft)

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Operational Requirements

Sub-Committee

to the

Executive Committee

TRANSMISSION SECURITY

The Operational Requirements Sub-Committee considered the Security Sub-Committee's report to the Executive Committee on Transmission Security.

2. It was noted that this was the first occasion on which the general subject of Transmission Security had been discussed at a UK/US Communications Security Conference. Although considerable difficulties in meeting the security ideals set forth in the above report by the Security Sub-Committee were foreseen, the Operational Requirements Sub-Committee endorsed the report and recommended that the action proposed in paragraph 3 of Appendix B of the Report of the report should be taken without delay.

3. With reference to paragraph 2g of the Security Sub-Committee's report it was noted that automatic traffic flow security was currently being provided in certain cases by the use of Apparatus 5 UCO No. 1.

It is noted that certain aspects of and [illegible] of the problems are under Should be integrated with the studies already under investigation by the respective UKUSA's & other bodies concerned

2nd November, 1953.

~~TOP SECRET~~

~~TOP SECRET~~ Copy No. 11

LCS(53)/OR/R(2)(FINAL)
9th November, 1953.

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Operational Requirements Sub-Committee on

Combined and NATO Requirements for Facsimile Security Equipments

and for Cryptographic Systems for Meteorological Traffic

A. Facsimile Security

1. The Sub-Committee took note that there would eventually be a combined UK - US requirement for Black/White facsimile transmission by secure means over long distance H.F. radio point-to-point circuits as well as by broadcasts. (There was no requirement in respect of NATO so far as could be stated at present).

2. CIFAX

a. It was noted that the question of combined technical standards for facsimile equipment was under consideration by the CAN-UK-US communications equipment panels, and whilst some agreements had been reached there were no complete combined standards for facsimile equipment. The question of combined CIFAX was therefore rather difficult at this stage. The following technical standards would have to be established before a combined specification for CIFAX could be drawn up:-

(1) Size of picture.
(2) Definition required.
(3) Index of co-operation of FAX equipment.
(4) Time allowed for transmission of a picture.
(5) Frequency band of radio Communications systems
(6) Type of transmission system.
(7) Crypto system.
(8) Communications plan for usage of CIFAX.

The Sub-Committee agreed that (1) through (5) were already covered by the CAN-UK-US J.C.-E.C. deliberations; but made the following recommendations on the remainder.

b. Type of Transmission System

Whilst it is understood that the J.C.-E.C.'s had already agreed that multi channel SCFM was the best method of transmission for CIFAX for other than short distances ground wave H.F. radio links, the Sub-Committee recommended that the Executive Committee should be asked to invite the Communications Equipment panels of the CAN-UK-US J.C.-E.C.'s to agree a technical specification for a multi channel SCFM transmission system for combined use in conjunction with CIFAX.

c. Type of Crypto System

The Sub-Committee noted that both the U.S. and the U.K. had specific projects for black/white CIFAX under test, but it was as yet too early to consider one to meet combined requirements. The only comment which could be made at this stage was that such a system must be reliable in operation and present no undue maintenance problems.

d. Communications plan for using CIFAX

The requirements of equipments and volume of traffic were estimated to be:-

U.K.

Air Ministry Meteorological Office

Some point-to-point circuits.

Single transmission broadcast on 3 frequencies each to 20-40 receivers.

64 pictures a day from each transmitter would be adequate.

Royal Navy

Some point-to-point circuits.

2 or more Broadcast systems each with 12-20 "receiving only" stations envisaged at the moment but a further requirement is possible.

64 pictures a day from each transmitter would be adequate.

The U.K. requirements would involve point-to-point circuits to North American and European Stations; but mainly broadcasts from Dunstable.

On the Continent a few score receivers would be necessary, all receiving continuous transmissions.

U.S.

Navy

8 point-to-point circuits.

Probably 7 broadcast stations each with 12-20 receivers.

48 pictures a day from each transmitter.

Air Force

The U.S.A.F. requirements involved up to ten continuous broadcast facilities each with approximately 20 "receiving only" stations.

There is also a requirement for up to a hundred point-to-point secure facsimile circuits.

3. There was a general requirement in the Navies to read broadcasts from both nations. In the Air Forces this was not so important but it was considered desirable to standardise equipment so as to make interworking possible if required.

/4.

844

4. The Sub-Committee recommend that reports of the trials carried out on Mountebank, AFSAJ 700 and AFSAX D 503 should be exchanged when available.

B. Cryptographic System for Meteorological Traffic

5. Statement of Requirements

The Sub-Committee reaffirmed the Combined and NATO requirements for weather controlled information transmitted by radio, as set out in the Report (WCS/R(2) FINAL) approved in the UK/US Communications Security Conference, 1952. These requirements are listed below:

a. Continental and Sub-Continental weather Broadcast via CW. (Off-line crypto-equipment needed.)

b. Weather portion of Naval general (admin.) broadcast. (Off-line crypto-equipment needed).

c. Theatre Operational Weather Information disseminated by Commands to tactical units. (Preferably same crypto principle used as in para. a.).

d. Continental and Sub-Continental exchange of Weather Data on RATT Pt to Pt circuits. (On-line crypto-equipment needed).

e. Collection of Data from Ground Reporting Stations by CW

(1) Intra-national only. No Combined and NATO requirement.

(2) Between Stations of different nations. (Off-line crypto-equipment needed. One-time pads will suffice where traffic load does not exceed 3000 groups per day). Same off-line crypto-system as for a. above.

f. Weather Reports for Aircraft

(1) Reconnaissance (Off-line cryptosystem. One-time pads will meet this requirement).

(2) Combatant mission - no special weather system required.

(3) Non-Combatant mission (preferably will be part of operational cryptosystem).

g. Weather Reports from Ground to Aircraft - (Includes requests for weather from aircraft).

Landing weather and IN-flight weather. OFF-line system needed. UCO has been accepted for Combined use on an interim basis for multi-seater aircraft.

6. Present Status

Papers have been introduced in the CAN-UK-US J.C.-E.C.'s covering requirements in a, b, c, e, f(1) and g above. These papers provide inter alia for the use of CCM as the off-line cryptosystem.

7. CCM and Met. Crypto Plan

As there was no objection to the use of operational rotors with MET Key Lists, it was agreed that, taking all factors into consideration, 1st July, 1954,

844

~~TOP SECRET~~

could be treated as a reasonable date by which CCM can be in position world-wide for Combined and NATO Meteorological traffic. For reasons briefly explained in the next para. however the Sub-Committee recommend that the Met crypto plan as outlined in para. 5 should so far as possible be implemented by 1st May, 1954.

8. Interim System

Consideration was given to the argument for an interim cypher system pending the introduction of CCM for MET in the event of war occurring during the intervening period. In this event intense aerial activity on both sides would be a feature of the early phases of a general war. It was therefore necessary that security should be provided for MET information. It was noted that the S.S. Frame system could be made available by the U.K. for this purpose, but the date by which the S.S. Frame system could be in position world-wide would be only a few weeks before the CCM. It is considered inadvisable to place an interim system in position for so short a time and moreover the distribution of the S.S. Frame would retard the distribution of the CCM. It is therefore recommended that all efforts should be concentrated on putting the CCM into position by the 1st May, 1954. It is noted that in the event of an emergency arising in the meantime, the S.S. Frame would still be available for issue to NATO with very little delay.

9. One-Time Pads

The Sub-Committee recommended that stocks of pads should be built up with a view to implementing the MET. Crypto plan by 1st May, 1953.

10. ON-LINE Cypher facilities

To provide such facilities for certain trunk RTT circuits shown in the integrated MET Communications Plan, approximately 30 duplex terminals in the Atlantic area alone should ideally be operated in Wartime. At the moment only 25 ASAM 2-1 machines can be made available (for non-synchronous operations). It is not advised that these should be used on-line on radio circuits but they can be used off-line with very little delay at the expense of additional handling effort at the terminals. They should be retained as an interim provision for an emergency although they are not a satisfactory method of handling the traffic; synchronous on-line equipment is considered essential.

The CAN-UK-US J.C.-E.C.'s are currently considering the detailed statement of the meteorological communications requirements prepared by the NATO Met. Committee. When these are agreed, the appropriate Communication Security panel of the J.C.-E.C.'s will make a more detailed recommendation as regards crypto-systems.

11. UCO

At present "UCO" is the only system available to meet the Combined and NATO requirement for the transmission of weather information to multi-seater aircraft in flight. It is recommended that stocks of daily letter scrambles should be made available to enable UCO to be in position by 1st May, 1954.