~~TOP SECRET~~

U.S

Copy No. 10

LCS(53)/OR/R(5) (Final)
9th November, 1953.

UK-US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Operational Requirements Sub-Committee to the Executive Committee

Security devices for I.F.F., Navigational Aids and Data Transmission Systems

1. I.F.F. Security Systems

a. The present combined UK/US agreements for I.F.F. systems envisage the use of S.I.F. with I.F.F. Mk. X as an identification system. Both U.S. and U.K. have studied these proposals from the security point of view.

b. The Sub-Committee recommend:-

(1) That the attention of the CAN-UK-US J.C.E.C.'s should be directed to the fact that the security agencies of both countries agree

(a) that the present proposal for using S.I.F. with I.F.F. Mk. X, with code changing on Mode I, is insecure as an identification system;

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

(2) That the CAN-UK-US J.C.E.C.'s be invited to restate the security requirements for a system to operate in conjunction with I.F.F. Mk. X. This specification should contain information about the degree of confidence in the identification required, and the amount of risk which would be acceptable.

(3) That when the security requirements have been received from the CAN-UK-US J.C.E.C.'s the cryptographic agencies of the U.S. and the U.K. make joint technical proposals for a new and secure I.F.F. system on the following basis:-

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

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

/2.

~~TOP SECRET~~

2. Navigational Aids and Data Transmission Systems

a. It was assumed that security systems for Navigational Aids and Data Transmission Systems might be required for two reasons:-

(1) To deny their use to an enemy in wartime

and (2) To prevent the enemy gaining any intelligence from their designed use by friendly forces.

b. No combined requirements for security systems for Navigational Aids had been formally submitted to either the U.S. or U.K. cryptographic agencies. Both agencies however, realised that such requirements might eventually be formulated, and had devoted some effort to theoretical studies of the possibilities of Security ideas for particular systems.

(1) In the U.S.

(a) On Navigational Aids, some theoretical studies had been undertaken under the General Research and development programme in N.S.A.

(b) On Data Transmission technical assistance had been given on specific projects under development in Service Laboratories.

(2) In the U.K.

A start had been made by inviting all Services to submit details of Navigational Aids in use or projected. This data had now been received and some amplification of specific items was being sought prior to further detailed study.

c. The Sub-Committee agreed that

(1) Neither the U.S. or U.K. cryptographic agencies were at this stage able to put forward any practical solution to these problems.

(2) The Executive Committee should take note that in both countries it was considered that insufficient effort was as yet available for the detailed studies of these problems even on a theoretical basis. Both Agencies would probably require an increase in personnel or an alteration in priorities if this was to be rectified.

(3) The entire field of I.F.F., Navigational Aids, Data Transmission, etc. represents a new field for which security must be provided. It appears that completely new cryptographic techniques will be required for it. Because of this and the peculiarity of the signals, the use of the signals and the stringency of size and weight factors, the development of the transmission portions, control portions, and security portions of these equipments will probably have to be done together. Therefore the attention of the J.C.E.C.'s should be directed to the necessity for requirements for these special equipments to be stated to the appropriate security agencies as soon as they are generated.

~~TOP SECRET~~

US

D/C

Copy No. 1

LCS(53)/OR/R(5) (Final Draft)
7th November, 1953.

UK-US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Operational Requirements Sub-Committee

to the Executive Committee

Security devices for I.F.F., Navigational Aids

and Data Transmission Systems

I. I.F.F. Security Systems

The present combined UK/US agreements for I.F.F. systems envisage the use of S.I.F. with I.F.F. Mk. X as an identification system. Both U.S. and U.K. have studied these proposals from the security point of view.

The Sub-Committee recommend:-

1. That the attention of the CAN-UK-US J.C.E.C.'s should be directed to the fact that the security agencies of both countries agree

(a) that the present proposal for using S.I.F. with I.F.F. Mk. X, with code changing on Mode I, is insecure as an identification system;

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

2. That the CAN-UK-US J.C.E.C.'s be invited to restate the security requirements for a system to operate in conjunction with I.F.F. Mk. X. This specification should contain information about the degree of confidence in the identification required, and the amount of risk which would be acceptable.

3. That when the security requirements have been received from the CAN-UK-US J.C.E.C.'s the cryptographic agencies of the U.S. and the U.K. make joint technical proposals for a new and secure I.F.F. system on the following basis:-

/(a)

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

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

II. Navigational Aids and Data Transmission Systems

1. It was assumed that security systems for Navigational Aids and Data Transmission Systems might be required for two reasons:-

(a) To deny their use to an enemy in wartime,

and (b) To prevent the enemy gaining any intelligence from their designed use by friendly forces.

2. No combined requirements for security systems for Navigational Aids had been formally submitted to either the U.S. or U.K. cryptographic agencies. Both agencies however, realised that such requirements might eventually be formulated, and had devoted some effort to theoretical studies of the possibilities of Security ideas for particular systems.

In the U.S.

On Navigational Aids, some theoretical studies had been undertaken under the General Research and development programme in N.S.A. On Data Transmission technical assistance had been given on specific projects under development in Service Laboratories.

In the U.K.

A start had been made by inviting all Services to submit details of Navigational Aids in use or projected. This data had now been received and some amplification of specific items was being sought prior to further detailed study.

/It

It was agreed that

(1) Neither the U.S. or U.K. cryptographic agencies were at this stage able to put forward any practical solution to these problems.

(2) The Executive Committee should take note that in both countries it was considered that insufficient effort was as yet available for the detailed studies of these problems even on a theoretical basis. Both Agencies would probably require an increase in personnel or an alteration in priorities if this was to be rectified.

(3) The entire field of I.F.F., Navigational Aids, Data Transmission, etc. represents a new field for which security must be provided. It appears that completely new cryptographic techniques will be required for it. Because of this and the peculiarity of the signals, the use of the signals and the stringency of size and weight factors, the development of the transmission portions, control portions, and security portions of these equipments will probably have to be done together. Therefore the attention of the J.C.E.C.'s should be directed to the necessity for requirements for these special equipments to be stated to the appropriate security agencies as soon as they are generated.