REF ID:A522915

~~SECRET.~~

LCS(53)/OR/R(1). (FINAL DRAFT). COPY NO: 30

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Operational Requirements Sub-Committee

to the

Executive Committee.

Expression of Security Requirements.

1. The Operational Requirements Sub-Committee recommend that using Services express their security requirements in accordance with the following:-

a. The proposed level of use.

b. The expected traffic load per day.

(1) Average.

(2) Maximum.

c. Message lengths.

(1) Expected average

(2) Required range.

d. Details of any special traffic peculiarities (Stereotypes, pro-formae, tabulators, etc.)

e. Procedural requirements.

(1) Acceptable length restrictions.

(2) Desired cryptoperiod.

(3) Acceptability of:

(a) Disguised message indicators.

(b) Bisection.

(c) Variable spacing.

(d) Paraphrasing.

f. The classifications of traffic to be passed in the system (Estimated proportion of Top Secret.)

/(g)

~~SECRET.~~

Declassified and approved for release by NSA on 05-27-2014 pursuant to E.O. 13526

REF ID:A522915

~~SECRET.~~



(g) The intelligence importance of the traffic to the enemy.

(1) Short term.

(2) Long term.

(h) Cryptonet requirements and likely number of holders per net.

(i) The physical security conditions.

(j) Operator training limitations and expected quality of operators.

2. This will enable a "confidence factor" to be calculated for the using Services by the security evaluators, if it is required. This may be defined as the odds against successful enemy cryptanalysis within a stated period of time.

3. Where it is desired by using Services to calculate confidence factors in advance, a statement of the acceptable confidence factor should accompany the statement of security requirements.

2nd November, 1953.