~~SECRET.~~

Copy No: 1

LCS(53)/N/R/1 (Final)

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953

Report of the Engineering Committee - Phase I
to the Executive Committee

1. In accordance with the recommendation of paragraph 11 c (1) of the Report to the British Chiefs of Staff and the U.S. Joint Chiefs of Staff of the UK/US Communications Security Conference held in Washington in May-June 1952, the Engineering Committee has prepared data sheets for each equipment available or under development, and has made recommendations on certain salient points. The recommendations which follow are based on observations made and informal discussions held during the fortnight reserved for this purpose prior to Phase I of the 1953 Conference.

2. The Engineering Committee viewed equipment where possible and held discussions on the following:

Literal Off-line Crypto Systems
On-line teletypewriter Crypto Systems
Ciphony Systems
Cifax Systems
Spurious Emissions which endanger Communications Security [SPEM]
Crypto Material Production Equipment
Security Systems for I.F.F. and Navigational Aids
General Review of new electronic techniques.

3. The major recommendations of the Engineering Committee are:

A. Future Combined Research and Development Effort

There is considerable similarity between the specific R & D projects being pursued by the U.K. and U.S. Although this means duplication of effort in some instances it is not necessarily wasteful duplication. On the contrary it assures protection of national interests, and the healthiness of independent lines of investigation. However, this very similarity offers an opportunity for effecting considerable economy of development resources. The Engineering Committee believes that with more specific guidance on operational requirements from the Service Departments, economy could be achieved. This guidance, it is felt, should be in the form of a directory of Combined and NATO Cryptographic security requirements. The Directory should include also listings of crypto-equipment and systems available or under development to meet the stated requirements.

It is recommended that the Executive Committee consider the desirability of preparing such a directory and the best method of effecting this.

B. Progress in Electronics

There have been significant advances in Electronics and Circuitry since the 1952 Conference. In the past, electronic techniques have, with few exceptions, been adopted only where the speed of operation would preclude the use of electromechanical methods. Electronic methods are now being explored for application to On-line Teletypewriter Cypher Systems and even to some off-line Literal Cypher Systems.

/It

~~SECRET.~~

~~SECRET.~~

It is recommended that the Service Departments be informed of this trend and of the fact that it will have a profound effect upon crypto-operations, supply, and maintenance as they are practised to-day. Of these changes, those which affect the training of maintenance personnel are probably the most difficult. Because of this, thought and planning should be started now by the Services if they are to be in a position to enjoy the full benefit of the advantages offered by electronic crypto-equipments when they become available.

C. Co-ordination of Cryptographic and Communications Equipment Development

The present practice of almost independent development of cryptographic equipment and certain forms of communications equipment has ~~usually~~ often led to incompatibility of one with the other. In order that compatibility may be achieved it is essential that such communications security as is required should be considered an integral part of the communications requirement at the time when the Staff and Operational Specifications and/or Military Characteristics are being formulated. This is necessary so that the cryptographic equipment may be designed to suit the requirements of the communications system or, where necessary, the communications equipment and practices may be adjusted to make possible the utilisation of an acceptable cryptographic system.

It is recommended that the necessary steps be taken to ensure that this course of action is adopted by all concerned.

D. Operating and Maintenance

The development authority must maintain close co-ordination with the User Services so that the operating and maintenance requirements are made known at all stages in the development. Thus, Users may weigh the need for the equipment against the maintenance and training requirements and, if necessary, the development authority may adjust the design to meet the operating and maintenance problem.

It is recommended that there be consultation between the development engineers and the Service engineers and communicators as early as possible in the process of development of each equipment in order to achieve these ends.

E. Spurious Emissions which endanger Communications Security (SPEM)

The Committee agree that radiation, conduction and induction from communication and crypto devices are very grave sources of insecurity.

Although investigations are by no means complete it is recommended that:-

(i) All cryptographic equipment using teletypewriter ancillaries and/or sequential signalling of clear text or key be considered insecure up to a distance of at least 200 ft. in any direction from the equipment, unless the equipment has been specially protected.

(ii) All crypto systems and ancillaries be investigated at high priority, to protect them and ensure that appropriate rules can be formulated for their use and siting.

(iii) Future equipments be designed to be free from such spurious emissions.

/F.

~~SECRET.~~

F. Future Engineering Discussions

The fortnight reserved before the Conference for visiting Establishments, viewing equipments and informal discussions between engineering experts has proved of very great value to the Engineers of the Service Departments. It is considered, however, that a better arrangement needs to be made for the Engineers from the Research and Development Establishments to obtain detailed information and to exchange views on techniques, etc.

It is recommended that:-

(i) The assignment, on a semi-permanent basis, of qualified technical liaison officers to the R & D establishments of one or both agencies should be considered.

(ii) Future Conferences should provide a preliminary phase to enable the Engineers and Communicators of the Service Departments to visit Establishments, view and discuss appropriate equipments which are available and under development.

(iii) There should be more frequent visits, independent of the formal Conferences, by engineers of both countries in small parties to discuss specific problems or equipments.

G. Exchange of Components and Models of Crypto Equipments

It is recommended that as a regular procedure each nation provide to the other, on an indefinite loan basis, for test and examination, engineering and first production models of components and equipments of mutual interest: and that if exchange is not practicable the equipment will be subjected to an agreed series of tests in the parent country.

[redacted] PL 86-36/50 USC 3605

Chairman.
Engineering Committee

8, Palmer Street,
London, S.W.1.

29th October, 1953.

~~SECRET.~~