ADD 3

18/3/33

PROJECT LOBSTER; NEW CRYPT COMPUTER

ADC

... Attached is a description of the various tasks I see necessary to complete our formal study of the requirement for a new CRYPT computer.

2. It is expected that all the tasks will require dialogue with C Branch personnel, particularly CHR.

3. However two of the envisaged tasks (tasks D and E), which will form the basis on which the whole requirement is justified, are clearly matters of C Branch expertise and policy.

4. Your advice on whether these tasks are an adequate specification of C Branch involvement in the study and how you wish them to be handled would be appreciated.

SM

1 March 1982

Copies to :

ADD
ADS
SMT

3A

Project LOBSTER - Task Assignments

Following are the initial tasks which I envisage are required to commence the Project LOBSTER study. I would expect that each task would result in a written report by the target dates established.

A. Benchmarks

Develop suitable benchmarks to measure the comparative speeds of the Cyber 175, Cray I, Cyber 7600 and Cyber 176 on computations typical of DSD's crypt processing requirements. Investigate possibility that NSA and GCHQ may be able to provide useful benchmarks. Liaise with NSA to obtain access to their machines to run the benchmarks. The benchmarks should also be produced in a form suitable for passing to equipment suppliers.

Responsibility: SMT2 **Target Date:** 1 July 82

B. Access to NSA Crypt Systems

Investigate the possibility of interim access to a FOLKLORE system at NSA if feasible, this could possibly provide a useful tool for evaluating and gaining expertise in FOLKLORE/IMP and programs of interest to DSD.

Responsibility: SM/SMT **Target Date:** Apr 82

C. IMP Support Under NOS/BE

IMP language support under NOS/BE would enable the use of IMP programs concurrent with existing Cyber processing and so retain unrestricted access to NOS/BE facilities whilst supporting the running of IMP programs.

However this proposal should be carefully studied to ascertain its technical feasibility, manpower resource requirements and the degree of compatibility which would actually be obtained with FOLKLORE supported IMP.

Responsibility: SMT2 **Target Date:** 1 May 82

D. Projected Processing Needs: Types and Volumes

A forecast of DSD crypt processing needs for the 80s is required, including possible new sources and identifying any special input device requirements.

Responsibility: C Branch **Target Date :** (1 July 82?)

3B

E. NSA and GCHQ Programs of Use to DSD

Investigate the availability of crypt programs at GCHQ and NSA of potential use to DSD. Quantify the number, size, languages, development effort potentially avoided at DSD and the improved implementation speed achievable.

Responsibility: CHR Target Date: 1 Sep 82?

F. Preliminary Survey of Commercially Available Systems

Conduct a survey of suitable currently available machines, their cost and building facility requirements.

Responsibility: SM/SMT Target Date: July 82

G. Computer Requirements

Establish the technical parameters of the machine required to meet crypt processing requirements:

- speed (total capacity and responsiveness)
- compatibility issues
- continued support or conversion of existing NOS/BE based fortran and assembler programs
- interactive facilities required
- relationship to other processing facilities and possibly other specialist front ends)
- assess the relative suitability of the architectures of various available commercial machine alternatives

Responsibility: SM/SMT Target Date: Dec 82