GOVERNMENT COMMUNICATIONS HEADQUARTERS,
OAKLEY, CHELTENHAM, GLOS.

[redacted]

[redacted]

Tel. : CHELTENHAM 55321.

DGC/5143.

18th December, 1954.

My dear John,

This is in answer to your letter of 20th October, 1954 to Joe Loehnis.

Strath has paid his visit to us. We all very much agree with your judgment that he is a "very worthwhile person". He is also a very nice one, and shrewd and well-informed into the bargain. I think that by the time he left he had at least modified his opinion on Colorob, though I would not go so far as to say that he was convinced that DSB ought to have one. One thing we certainly made clear to him, namely, that if Australia has a Colorob, it is our view that DSB (and not Supply) should provide the staff to analyse cryptanalytic needs in terms of machine processes, and that in consequence Supply need not fear that they will be committed to any specialist staff other than maintenance engineers.

We for our part have taken the opportunity to review the whole problem. This has taken a lot of time and has involved a certain amount of correspondence with Washington about NSA work [redacted] so that the reply to your letter is a bit belated; I hope however that it will reach you before Strath gets home.

Here, then, is a restatement of our views:

1. The main justification for having a Colorob at DSB is to be found in its wartime applications.

2. DSB cannot do the work [redacted] Hagelin as specified in the Tripartite Conference report* without a high speed machine, and Colorob would provide the machine facilities required. It is however noteworthy that the present NSA machine effort [redacted] considerably exceeds the capacity of one Colorob; you could certainly use one profitably whole-time!

3. The work [redacted] Hagelin[x] should provide an adequate field to enable DSB to build up a cadre of experienced cryptanalysts and Colorob programmers. Without such a cadre Colorob would be no more than a white elephant, in peace or in war.

4. There is no crypt problem currently handled at DSB or likely to arise on any DSB peace-time task, other than [redacted], for which rapid analytic machinery is required.

5. If DSB expand their crypt effort on Hagelin, recruit and train machine programmers and machine operators and

/acquire

*MTC/53/1 Appendix B, Annexure 3, paragraph 12.

[x] This of course presupposes that the [redacted] go on using their existing machines. The firm of Hagelin has recently launched a new version of their machine which if really well used is likely to be unbreakable. [redacted]

[redacted]

[redacted]

acquire a Colorob, they may expect to effect some improvements on the present service of [redacted] But they must not hope for too much too quickly.

(a) I gather from MIO here that the time-lag in production [redacted] is a source of dissatisfaction to Australian Customers. So far as I can make out there are three causes of this long delay:

(i) No start can be made on any [redacted] until either a depth is given or a long message sent. Here we can do nothing but wait, often for a month or so out of three months' life of a machine.

(ii) When the favourable message or messages have been intercepted they must be delivered to the cryptanalysts [redacted] which may take several weeks. This is a quite separate problem involving such matters as cable scrutiny [redacted]

(iii) It may take [redacted] to solve a new machine. [redacted] tried machines on [redacted] and given them up as no good. The only remedy seems to be more and better linguists in the Crypt section*.

Having a Colorob will make no difference to any of these causes of delay, but not having one would lead to considerable additional delay in setting messages.

(b) A number of [redacted] are still unsolved, although [redacted] given high priority to [redacted] have just about all the [redacted] they could possibly ask for. We think it likely that a good crypt mathematician taking a fresh look at the whole problem would see a new approach, since there seems to be enough data (in some cases at least) to make solution possible. We would go so far as to say [redacted] seems to be getting poorish value for the gigantic machine effort expended, and it would not surprise us unduly if one Colorob really expertly used might not, in some respects, do better.

(6) If DSB orders a Colorob now they should also set about recruiting at least one good Scientific Officer with a first-class Honours degree in mathematics, to be trained at GCHQ as a "programmer". This is additional to the training of a machine cryptanalyst[xx], and I must warn you that we cannot undertake to provide a scientist with the right

/experience

* It does not look very likely [redacted] would be able to contribute very much by way of "loaning [redacted] to work as integrated members of DSB" (MTC/53/1, Appendix B, Annexure 3, paragraph 12).

xx I hear Tony Eastway has been selected for this; we shall of course be very glad to see him here again.

GOVERNMENT COMMUNICATIONS HEADQUARTERS,
OAKLEY, CHELTENHAM, GLOS.

Tel. : CHELTENHAM 55321.

DGC/5143.

TOP SECRET [redacted] FROTH

experience from GCHQ, as suggested in your letter; we have not nearly enough people of this kind to meet our own needs. This scientist should be in training here while the DSB Colorob is being built and should go with the machine to Australia.

(7) Finally we would like to say once again it is the cadre of expert machine staff that makes all the difference. It would be impossible to build up such a cadre without at least one rapid analytic machine but all the machines in the world would be no good without trained bodies to run them.

Yours ever
[signature]

P.S. The latest news of [redacted] is quite satisfactory. He has not yet been moved from Wycombe hospital, & I gather can't be moved till after Christmas & they haven't yet been able to set the broken jaw. Serena has just made him a grandfather & all is well with her & a nice little boy. [redacted] he cooed us with a bit of cheerful news. Thank heaven he is alive, it was a fearful smash.

J.O.H. Burrough, Esq.,
Senior United Kingdom Officer,
D.S.B.

P.P.S. I'm afraid that this letter chills her bones me some time & combs won't reach for Xmas. But do tell Ralph, & Mrs Thompson & the Flemings & Ricky & all the DSB folks that I was wishing them a happy Christmas & new year.

TOP SECRET [redacted] FROTH