Mr 7# Here is a copy of the note I made of what you were just talking to me about. JH

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

From: G.C.H.Q. DTG: 011636Z/December '53

To: S.L.O., Washington

1. The first step is the preparation of an Agenda. The following points must be taken into consideration in producing it:-

(a) We cannot hope to cover every eventuality in advance: the best way of eliciting and developing certain points must be left to the discretion of the Delegates on the spot within our agreed limits of disclosure.

(b) We know that the French have shown themselves willing to seek advice on cryptography from U.K. and U.S. and that they have confidence that we are competent and dis-interested advisers. Provided that nothing happens to destroy the French confidence in us we may legitimately expect them to be cooperative: if they are not, the negotiations as at present planned will fail and only an entirely different approach, such as the 'shock tactics' that we abandoned at the June Conference, could hope to succeed.

(c) The French should be encouraged to bring forward any item of U.K. or U.S. insecurity known to them for inclusion in the discussions.

(d) If the U.K. and U.S. delegates were able to disclose all the detailed knowledge that they possess it would be fairly easy to show that the agenda ought to include [redacted] Some suggestions on methods of approach are given below.

2. There are two documents available which may be put before the French, viz: the aide memoire to be left by the Ambassadors and the 'List of Dangerous Practices' prepared for later use with NATO countries outside the Standing Group. I suggest that we cannot do better than use these documents as the agenda for the first meeting at which a detailed programme will be drawn up.

3. Methods of approach to discussion of individual systems:

EO 3.3(h)(2)
PL 86-36/50 USC 3605

(a) Starting with the 'List of Dangerous Practices' we would strive to reach a measure of common agreement on systems that are fundamentally insecure and practices that must be forbidden. We would at this stage seek to get the list accepted in principle or perhaps amplified from the French side. We will not of course at this or any other stage allow the meeting to discuss the practices of any nation not represented.

~~TOP SECRET FROTH~~

TOP SECRET FROTH

(b) In proceeding from this somewhat theoretical discussion to practical issues we may hope to elicit from the French at least something of what we already know by referring to our own experience in COMSEC and by mentioning some of the previous occasions on which we have discussed COMSEC with them.

(c) We must endeavour tactfully to induce the French to discuss at least the following:-

I. The machine systems T52, M209 and B211.
II. Non-one-time additive Hand Systems.
III. Uncyphered codes, and codes cyphered by substitution.
IV. Future developments, T53, Gretener, etc.

4. The T52, might be introduced into the agenda by saying that our experience of on-line cyphers had taught us that these were exceptionally liable to compromise through the carelessness or the indiscipline of the personnel who operate them.

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(b) Transmissions must be monitored and a record must be kept of settings used. Operators must be made to check one another i.e. a receiving operator must be told to refuse to work if offered a setting already used, or share in the responsibility for the violation.

[redacted]

5. M209 can be introduced by an enquiry about the modification demonstrated in 1951 and by drawing attention to the paragraph on HAGELIN systems in the 'List of Dangerous Practices'.

[redacted]

(d) In either event we must expect the French to confront us with the wartime assessments and we shall be forced to dissent from them.

7. Additive systems may be discussed in the light of our wartime experience.

(a) Monitoring, and collection of records of indicators used, showed how easily a system could become overloaded.

(b) Similarly, even if a system was not carrying a greater load than it was designed to carry, the perversity of operators would lead to local overloading of parts of the recypher table.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(c) As a result of these experiences we had come to the view that only one-time additive systems were satisfactory; other additive systems could be recommended only if extraordinary precautions were taken and the traffic load carefully controlled, and were fit only for small volumes of traffic.

8. On uncyphered codes and other low grade systems we might say that we had long ago abolished all [redacted] economy use with unclassified messages.

9. Future developments at least can be discussed without any difficulty [redacted] but the following points should be borne in mind:- OGA

(a) [redacted]

(b) The following U.K. or U.S. cryptoprinciples may be discussed:

I. The U.K. method of making one time pads by Hollerith.

II. The U.K. method of making random tape by Donald Duck, and the standards and procedures used for checking.

III. All one time tape devices.

IV. Circuit Mercury. This is not to be recommended to the French but they may well take the opportunity of the Tripartite discussions to return to the charge, having not had any answer to their earlier questions.

V. Portex, AFSAM 17 and AFSAM 9.

VI. Any system already cleared for NATO.