28 May 1953

~~TOP SECRET~~ ~~CANO~~

~~TOP SECRET~~
SECURITY INFORMATION

COMMENTS ON [redacted] POSITION PAPER

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

SECURITY INFORMATION

1. The subject paper is noteworthy not so much for its convincing nature, as for its evidence of a completely crystalized and rigid [redacted] position.

2. The portions dealing with mechanism can be ignored at this time, since they are secondary to the main question which is whether or not this step should be taken.

3. It appears from the paper as a whole that the U.K. is convinced:

A. That the insecurity of [redacted] is of more value to Russia than the resultant [redacted] is to the [redacted] and U.S.

B. That Russia could obtain the information [redacted] by no other means.

C. That this requires that we unequivocally sacrifice all [redacted] "(probably forever)" without further delay.

4. Point 3A above is elaborated upon at length in Appendix A, in a survey somewhat similar to that prepared by the AdHoc Committee of USCIB. The surveys are different in that theirs is based primarily on [redacted] products and ours on [redacted] products, and in the lack of any specific span of time in the [redacted] study whereas the U.S. study covered a six month period. Examination of cited examples reveals that their selection is considerably less rigid in terms of what is damaging. I think it probable that examination of the complete texts would reveal many instances of messages which sound serious in the extract but are rather trivial in the whole. Some are highly questionable even from the extract, as for example:

Annexure 2	item	4c
		4d
		4e
		4f
		5b
		5c (30 Jan 53.)
		6b
		6d
Annexure 4	item	4c
Annexure 6	item	4c
Annexure 7	item	3b

Nevertheless there is no doubt that a quantitatively small but nevertheless real leakage of intelligence is taking place. With respect to

[redacted] goes so far as to state that the amount is small. In this and in the appraisal of potential, the [redacted] are essentially agreed. The divergences are in estimates of degree.

5. Point 3B is the fundamental questionmark in the [redacted] This statement made without qualification or further comment in any form represents an assumption rather than a fact. This assumption runs counter to the known:

a. Communist infiltration of [redacted] and other [redacted] nations.

b. Elaborate public press and radio reporting of all [redacted] nations - particularly the U.S.

c. Recent oral report by [redacted]

6. Point 3B is essential to the U.K. position, since unless it is very nearly true, the course of action which the [redacted] insists upon would mean that Point 3C would be a burnt offering to an unresponsive deity. In addition if 3C is untrue to the extent that our attempts to inform the [redacted] in their turn, we would hand the USSR a picture of our own cryptographic (and, by inference, cryptanalytic) abilities.

7. The fundamental problem is not answered by the [redacted] paper. It remains a cold fact that someone with the requisite authority must make a command decision in which only part of the factors are known, a few can be guessed at and the remainder are hidden in the future:

a. Known - [redacted] are [redacted] to us
   Infer - They are also [redacted] against the USSR

b. Known - The quantitative leakage is not dramatic as of now
   Infer - It could grow worse - particularly in war

c. Known - Western open sources leave relatively little work for USSR intelligence as of now
   Infer - We might not cut off much intelligence by [redacted] ciphers

d. Known - USSR espionage of all types is very widespread and quite effective
   Infer - We might not accomplish much and might have disclosed a fair amount of [redacted]

e. Known - [redacted] is of value to us if not of dominant importance
   Infer - Who can judge its value to USSR?

~~U.S. EYES ONLY~~ ~~TOP SECRET~~ ~~CANOE~~

~~TOP SECRET~~
SECURITY INFORMATION

QUERY ? - Will one or more [redacted] go communist? [redacted]

" ? - Will at least the elements of existing cryptography remain if they were forced into [redacted]

" ? - Will we then want to read them?

" ? - Will we one day get intelligence vital to us in our position as leader of the Western block? Will we perhaps get warning of defection?

8. In one sense the die is cast. All we can do is control the speed of the eventual loss. When modern devises were given [redacted] by the [redacted] and [redacted] we set in motion an inevitable [redacted] This process will be relatively slow. We can accelerate this or let nature take its course. The decision must weigh the possible gain against the accelerated loss.

a. One final thought: If we are going to do anything more at this moment, let us improve the COMSEC only of those of our [redacted] partners of whose constancy we feel more or less certain and whose COMSEC needs improvement. For example: [redacted]

L. E. SHINN

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

~~TOP SECRET~~ ~~CANOE~~

~~U.S. EYES ONLY~~

If we are going to do anything more at this moment,

9. One final thought: let us improve the COMSEC only of those [redacted] of whose constancy we feel more or less certain and whose COMSEC needs improvement. For example: [redacted]

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

L. E. SHINN

~~TOP SECRET CANOE~~

COMMENTS ON [ ] POSITION PAPER ~~TOP SECRET~~ SECURITY INFORMATION

1. The subject paper is noteworthy not so much for its convincing nature, as for its evidence of a completely crystalized and rigid [ ] position.

2. The portions dealing with mechanism can be ignored at this time, since they are secondary to the main question which is whether or not this step should be taken.

3. It appears from the paper as a whole that the U.K. is convinced:

A. That the insecurity of [ ] is of more value to Russia than the resultant [ ] is to the [ ] and U.S.

B. That Russia could obtain the information [ ] by no other means.

C. That this requires that we unequivocally sacrifice all [ ] "(probably forever)" without further delay.

EO 3.3(h)(2)
PL 86-36/50 USC 360

4. Point 3A above is elaborated upon at length in Appendix A, in a survey somewhat similar to that prepared by the AdHoc Committee of USCIB. The surveys are different in that theirs is based primarily on [ ] products and ours on [ ] products, and in the lack of any specific span of time in the [ ] study whereas the U.S. study covered a six month period. Examination of cited examples reveals that their selection is considerably less rigid in terms of what is damaging. I think it probable that examination of the complete texts would reveal many instances of messages which sound serious in the extract but are rather trivial in the whole. Some are highly questionable even from the extract, as for example:

Annexure 2 item 4c
4d
4e
4f
5b
5c (30 Jan 53.)
6b
6d
Annexure 4 item 4c
Annexure 6 item 4c
Annexure 7 item 3b

Nevertheless there is no doubt that a quantitatively small but nevertheless real leakage of intelligence is taking place. With respect to

[ ]

~~TOP SECRET CANOE~~

~~TOP SECRET~~
SECURITY INFORMATION

[redacted] goes so far as to state that the amount is small. In this and in the appraisal of potential, the [redacted] are essentially agreed. The divergences are in estimates of degree.

5. Point 3B is the fundamental questionmark in the [redacted] This statement made without qualification or further comment in any form represents an assumption rather than a fact. This assumption runs counter to the known:

a. Communist infiltration of [redacted] and other [redacted] nations.

b. Elaborate public press and radio reporting of all [redacted] nations - particularly the U.S.

c. Recent oral report by [redacted]

6. Point 3B is essential to the [redacted] since unless it is very nearly true, the course of action which the [redacted] insists upon would mean that Point 3C would be a burnt offering to an unresponsive deity. In addition if 3C is untrue to the extent that our attempts to inform the [redacted] leaked in their turn, we would hand the USSR a picture of our own cryptographic (and by inference, cryptanalytic) abilities.

7. The fundamental problem is not answered by the [redacted] paper. It remains a cold fact that someone with the requisite authority must make a command decision in which only part of the factors are known, a few can be guessed at and the remainder are hidden in the future:

a. Known - [redacted] are [redacted] to us
   Infer - They are also [redacted] against the USSR

b. Known - The quantitative leakage is not dramatic as of now
   Infer - It could grow worse - particularly in war

c. Known - Western open sources leave relatively little work for USSR intelligence as of now
   Infer - We might not cut off much intelligence by securing [redacted]

d. Known - USSR espionage of all types is very widespread and quite effective
   Infer - We might not accomplish much and might have disclosed a fair amount of [redacted]

e. Known - [redacted] is of value to us if not of dominant importance
   Infer - Who can judge its value to USSR?

[redacted]

~~TOP SECRET CANOE~~

QUERY ? - Will one or more [redacted] go communist? [redacted]

" ? - Will at least the elements of existing cryptography remain if they were forced into [redacted]

" ? - Will we then want to read them?

" ? - Will we one day get intelligence vital to us in our position as leader of the Western block? Will we perhaps get warning of defection?

8. In one sense the die is cast. All we can do is control the speed of the eventual loss. When modern devices were given [redacted] by the [redacted] and [redacted] we set in motion an inevitable loss of [redacted] This process will be relatively slow. We can accelerate this or let nature take its course. The decision must weigh the possible gain against the accelerated loss.

a. One final thought: If we are going to do anything more at this moment, let us improve the COMSEC only of those of our [redacted] of whose constancy we feel more or less certain and whose COMSEC needs improvement. For example: [redacted]

L. E. SHINN

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

[redacted]