

~~TOP SECRET CANOE~~

~~TOP SECRET ACORN~~

REPORT

OF THE

U.K. - U.S. CONFERENCE ON SECURITY OF FRENCH COMMUNICATIONS
HELD AT WASHINGTON, 1 MAY - 14 MAY, 1951

*Extracts
only*

THE PROBLEM



- b. To assess the advantages and disadvantages of such an approach;
- c. To develop, if an approach should be made:
 - (1) a specific plan for improving the security of French communications, and
 - (2) a specific program for approaching the French Government.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

- 2. See Enclosure "B".


CONCLUSIONS

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

- 3. It is concluded that:



*Top
Conf*

- b. In view of the facts that -
 - (1) the U.K. and the U.S. Governments, through the mechanism of NATO  have initiated action which is expected to correct in large measure the insecurity of the important cryptocommunications of the French Armed Services; and
 - (2) any correction of the remaining important areas of insecurity of the cryptocommunications of the French Armed Services would

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

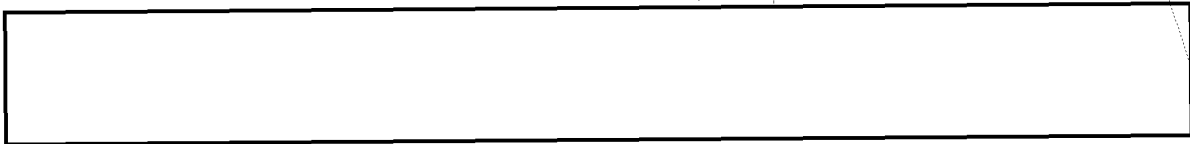
*Exp
Conf*



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



any direct approach to the French Government should be restricted in scope to the improvement of the security of the cryptocommunications of the French M.F.A.

c. The Cryptographic Service of the French M.F.A. does not possess the necessary cryptanalytic knowledge to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed.

Tech

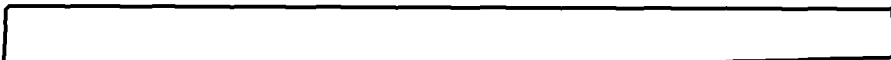
d. This situation can be improved only by a drastic and expensive reorganization of the Cryptographic Service of the French M.F.A. and appropriate replacement of its cryptographic systems and practices.

Tech

e. In order to assure a realization by the French M.F.A. of the necessity for such a drastic overhaul of cryptographic systems and practices it will be necessary to bring the situation to the attention of the M.F.A. in a manner so dramatic as to shock that Ministry into taking speedy and effective action.

*Ext
142*

f. If a shock of the degree necessary to produce effective action were possible



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



this type of approach to the French would be most advisable; however, for reasons set forth in paragraphs 25 and 26 of Enclosure "B" (TAB A), an approach of this sort would be inadequate, and an approach involving such revelation must therefore be employed, with concomitant risks arising from general insecurity in the French Government.

*at end
of
Cond*

g. At present the French Government is infiltrated with Communists and other disloyal or untrustworthy personnel, is subject to violent internal dissensions, and is careless of its own security to a degree where its classified information is seriously in danger of leakage.

Intell

h. Although direct evidence is lacking that Communists in French Government positions and U.S.S.R. agents have passed classified information in volume to the U.S.S.R., such passage of information must be assumed.

Int

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

i. The principal risks to the U.K. and the U.S. Governments in any approach to the French Government on the subject of the insecurity of its communications are:

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



Whole 9P
②

- (3) Disadvantageous political repercussions;
- (4) Pressure from the French for [redacted] collaboration.

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

j. Provided the conditions set forth in paragraphs 46 through 48 of Enclosure "B" (TAB B) for minimizing these risks can be met, an approach to the French M.F.A. is warranted.

John

k. Since the report of the Tripartite Group now studying the internal security of the French Government may well add to our knowledge in this regard, any approach to the French M.F.A. should be deferred pending consideration of that report.

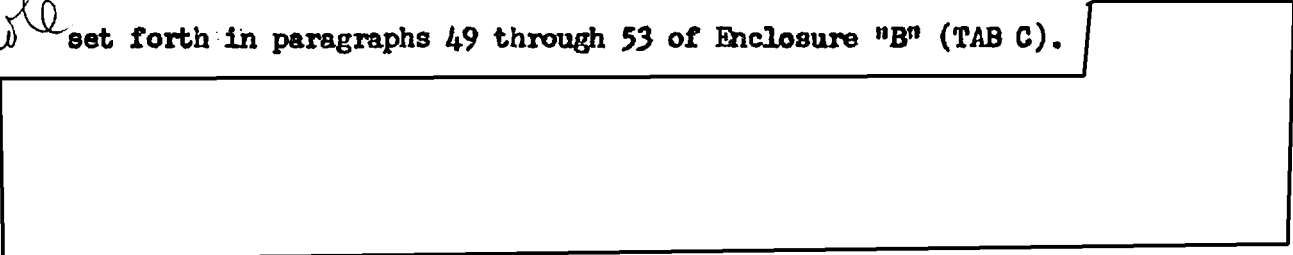
EO 3.3(h)(2)
PL 86-36/50 USC 3605

l. The urgency for improving the security of French [redacted] communications is such that a program to this end should be undertaken as soon as possible.

Int + Tech

m. The specific technical plan for the replacement of insecure cryptographic systems and practices of the French M.F.A. (set forth in Enclosure "A") should be presented to that Ministry in accordance with the approach set forth in paragraphs 49 through 53 of Enclosure "B" (TAB C).

Whole



n. Implementation of the plan will require the long-term loan to the French of a limited amount of U.K./U.S. cryptographic equipment. (This loan should consist initially of about 20 Combined Cipher Machines (CCM); subsequently 60 additional CCM should be ear-marked for this purpose, the latter being phased in consonance with NATO needs.)

For later consideration
②

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~

o. This problem should be kept under continuous review until a decision to approach the French has been made and the plan has been implemented.

RECOMMENDATIONS

4. It is recommended that:

- a. The above conclusions be approved;
- b. The proposed approach and plan be implemented when LSIB and USCIB have agreed that the requisite conditions have been met;
- c. The respective Chairmen of LSIB and USCIB and/or their nominees visit Paris in order to brief the U.K. and the U.S. Ambassadors and also to participate as required;
- d. LSIB and USCIB keep this problem under continuous review, and take such implementing action as may be agreed to be necessary;
- e. The U.K. Government provide eight and the U.S. Government twelve of the twenty CCMs required for initial implementation of the cryptographic plan, and that the additional sixty CCMs be provided by the two Governments in a program phased in consonance with their respective NATO commitments.

~~TOP SECRET CANOE~~

TAB "A"

EO 3.3(h)(2)
PL 86-36/50 USC 3605APPROACH TO THE FRENCH [REDACTED]

25. An approach to the French [REDACTED] has been considered, such an approach to be restricted to offering the French M.F.A. cryptographic material, including machines, [REDACTED]

26. Such an approach is deemed inadvisable for the following reasons:

a. The impact on the French is likely to be too feeble to effect the desired result. A drastic overhaul of the Cryptographic Service of the French M.F.A. is needed and this would require the allocation of additional funds which would probably not be forthcoming unless the French receive a major shock.

b. Even if the French acquiesced, there would, in the absence of assurances of improved security, remain the possibility of the U.S.S.R. acquiring the necessary cryptographic materials through Method 2.*

c. Any half hearted approach might prejudice a later approach based [REDACTED] furthermore, any approach by stages might lay the U.K. and the U.S. Governments open to French accusations of insincerity.

d. Acceptance by the French M.F.A. of participation by U.K./U.S. experts in the necessary drastic reorganization of its Cryptographic Service would not be likely to follow this approach.

e. The necessary number of cipher machines for this purpose is not available to meet French needs. Even if they were available, it could be anticipated that other NATO countries would make similar demands which could not be met.

*By obtaining physical possession of the cryptomaterial (key lists, code books, etc.) necessary for direct reading of the intercepted traffic.

~~TOP SECRET CANOE~~

CONDITIONS GOVERNING AN APPROACH TO THE FRENCH

46. In order to induce the French M.F.A. to undertake the drastic overhaul required for real improvement in its communications security, any U.K. or U.S. approach should be calculated to shock the Ministry into making a major effort. It is considered that the only effective and practicable shock

[Redacted]

47. Revelation [Redacted] entails such grave risks that it should be subject to the conditions outlined below:

a. Prior to the initial approach there must be valid indications that the French M.F.A. and those other French Government Departments and Agencies which have access to M.F.A. communications containing information handled on a classified basis by the U.K. or the U.S. Governments have the intent and capability to establish arrangements to protect this information; these arrangements must be sufficient, in the agreed opinion of the U.K. and the U.S. Governments, to warrant making an initial approach.

b. The initial approach must be made at a point of contact in the French M.F.A., which contact is discreet, reliable, and at a level of sufficient authority. This contact should be informed:

- (1)
- (2)

[Redacted]

- (3) that, should he not believe this statement, a demonstration will be given to his experts provided he will give assurances that his Ministry will:
 - (a) undertake an energetic program for reorganization of its Cryptographic Service and appropriate replacement of its present cryptographic systems and practices;
 - (b) accept without qualification and promulgate U.K./U.S. essential standards of security in each phase and aspect of the program;
 - (c) accept direct U.K./U.S. participation in executing the program, including participation on a working level by representatives qualified in the field of general security as well as all aspects of communications security.

~~TOP SECRET CANOE~~

~~TOP SECRET ACORN~~

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

TAB "B" CONTINUED

c. Should [redacted]

be unnecessary to convince the contact as to the [redacted]

[redacted] nevertheless, before any further steps in the program are undertaken,

the assurances set forth in paragraph b(3) must still be obtained.

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

48. In informing the French M.F.A. of details [redacted] of its

cryptographic systems, it is essential that as little information as possible

be divulged [redacted]

[redacted] These should be selected so as to reveal the minimum amount of

technical information, which should be restricted to the level of [redacted]

[redacted] systems. If any disclosure of [redacted] information relating to

[redacted] should be found necessary in order to obtain French

acceptance to the conditions specified in paragraph 47b, such disclosure will

not be made without prior agreement between the U.K. and the U.S. Governments.

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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~TAB "C"MEANS OF APPROACH

49. An initial approach to the M.F.A. at a level of sufficient authority offers a choice between the Minister and the Secretary-General. It is considered that the latter would be the more suitable point of initial approach for the following reasons:

- a. The Secretary-General is a permanent official, while the Minister is liable to replacement;
- b. As a Department official, the Secretary-General is more likely than the Minister to take a comprehensive and continuous view of the problem;
- c. The outstanding personality and known reliability of the Secretary-General, M. Alexandre Parodi, are believed to be such as to offer good prospects of effective implementation of the U.K./U.S. plan.

50. All subsequent widening of the circle of discussion will require precise definition and prior U.K./U.S. agreement.

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

51. The various risks arising [redacted] and particularly the [redacted] require that [redacted] but not both, the logical nominee being the U.K. [redacted] the French have been associated in the past.

52. There would be distinct advantages in a U.K./U.S. joint approach based on joint consultation and joint recommendations in the light of the [redacted] In view of the fact that a considerable effort on the part of the French is required, the maximum available pressure must be exerted.

53. Inasmuch as the U.K. and the U.S. Ambassadors in Paris have already been apprised of this problem and in view of their official positions, it is logical that they should make the initial approach to M. Parodi.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

Extracts only

~~TOP SECRET ACORN~~

REPORT

OF THE

U.K. - U.S. CONFERENCE ON SECURITY OF FRENCH COMMUNICATIONS

HOLD AT WASHINGTON, 1 MAY - 14 MAY, 1951

THE PROBLEM

- 1. To consider the insecurity of French Government Communications -
 - a. To determine whether the French Government should be approached with a view to improving its communications security, especially that of the Ministry of Foreign Affairs (M.F.A.);
 - b. To assess the advantages and disadvantages of such an approach;
 - c. To develop, if an approach should be made:
 - (1) a specific plan for improving the security of French communications, and
 - (2) a specific program for approaching the French Government.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

- 2. See Enclosure "B".


CONCLUSIONS

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

- 3. It is concluded that:



b. In view of the facts that -

- (1) the U.K. and the U.S. Governments, through the mechanism of NATO  have initiated action which is expected to correct in large measure the insecurity of the important cryptocommunications of the French Armed Services; and

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

- (2) any correction of the remaining important areas of insecurity of the cryptocommunications of the French Armed Services would



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~EO 3.3(h)(2)
PL 86-36/50 USC 3605

[REDACTED]

any direct approach to the French Government should be restricted in scope to the improvement of the security of the cryptocommunications of the French M.F.A.

c. The Cryptographic Service of the French M.F.A. does not possess the necessary cryptanalytic knowledge to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed.

d. This situation can be improved only by a drastic and expensive reorganization of the Cryptographic Service of the French M.F.A. and appropriate replacement of its cryptographic systems and practices.

e. In order to assure a realization by the French M.F.A. of the necessity for such a drastic overhaul of cryptographic systems and practices it will be necessary to bring the situation to the attention of the M.F.A. in a manner so dramatic as to shock that Ministry into taking speedy and effective action.

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

f. If a shock of the degree necessary to produce effective action were possible [REDACTED]

[REDACTED] this type of approach to the French would be most advisable; however, for reasons set forth in paragraphs 25 and 26 of Enclosure "B" (TAB A), an approach of this sort would be inadequate, and an approach involving such revelation must therefore be employed, with concomitant risks arising from general insecurity in the French Government.

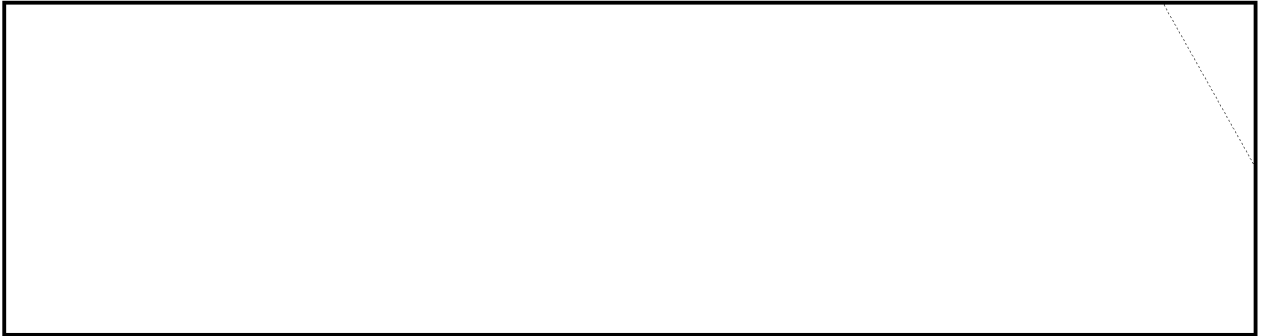
g. At present the French Government is infiltrated with Communists and other disloyal or untrustworthy personnel, is subject to violent internal dissensions, and is careless of its own security to a degree where its classified information is seriously in danger of leakage.

h. Although direct evidence is lacking that Communists in French Government positions and U.S.S.R. agents have passed classified information in volume to the U.S.S.R., such passage of information must be assumed.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~

i. The principal risks to the U.K. and the U.S. Governments in any approach to the French Government on the subject of the insecurity of its communications are: EO 3.3(h)(2)
PL 86-36/50 USC 3605



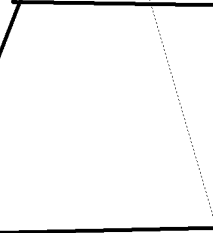
(3) Disadvantageous political repercussions;

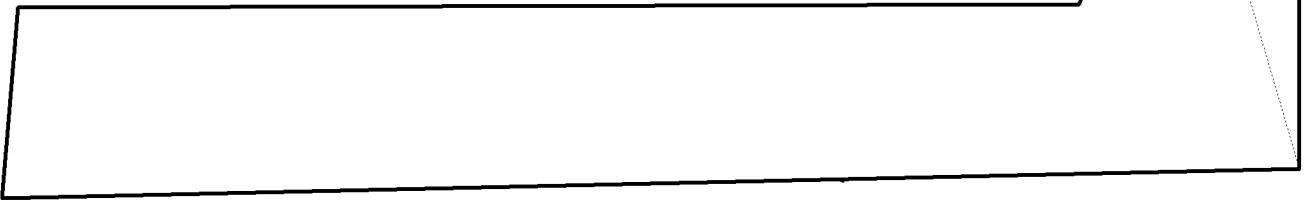
(4) Pressure from the French for collaboration. EO 3.3(h)(2)
PL 86-36/50 USC 3605

j. Provided the conditions set forth in paragraphs 46 through 48 of Enclosure "B" (TAB B) for minimizing these risks can be met, an approach to the French M.F.A. is warranted.

k. Since the report of the Tripartite Group now studying the internal security of the French Government may well add to our knowledge in this regard, any approach to the French M.F.A. should be deferred pending consideration of that report.

l. The urgency for improving the security of French communications is such that a program to this end should be undertaken as soon as possible. EO 3.3(h)(2)
PL 86-36/50 USC 3605

m. The specific technical plan for the replacement of insecure cryptographic systems and practices of the French M.F.A. (set forth in Enclosure "A") should be presented to that Ministry in accordance with the approach set forth in paragraphs 49 through 53 of Enclosure "B" (TAB C). 



n. Implementation of the plan will require the long-term loan to the French of a limited amount of U.K./U.S. cryptographic equipment. (This loan should consist initially of about 20 Combined Cipher Machines (CCM); subsequently 60 additional CCM should be ear-marked for this purpose, the latter being phased in consonance with NATO needs.)

- 3 -

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~

o. This problem should be kept under continuous review until a decision to approach the French has been made and the plan has been implemented.

RECOMMENDATIONS

4. It is recommended that:

a. The above conclusions be approved;

b. The proposed approach and plan be implemented when LSIB and USCIB have agreed that the requisite conditions have been met;

c. The respective Chairmen of LSIB and USCIB and/or their nominees visit Paris in order to brief the U.K. and the U.S. Ambassadors and also to participate as required;

d. LSIB and USCIB keep this problem under continuous review, and take such implementing action as may be agreed to be necessary;

e. The U.K. Government provide eight and the U.S. Government twelve of the twenty CCMs required for initial implementation of the cryptographic plan, and that the additional sixty CCMs be provided by the two Governments in a program phased in consonance with their respective NATO commitments.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~EO 3.3(h)(2)
PL 86-36/50 USC 3605

TAB "A"

APPROACH TO THE FRENCH

25. An approach to the French [redacted] has been considered, such an approach to be restricted to offering the French M.F.A. cryptographic material, including machines, [redacted]

26. Such an approach is deemed inadvisable for the following reasons:

a. The impact on the French is likely to be too feeble to effect the desired result. A drastic overhaul of the Cryptographic Service of the French M.F.A. is needed and this would require the allocation of additional funds which would probably not be forthcoming unless the French receive a major shock.

b. Even if the French acquiesced, there would, in the absence of assurances of improved security, remain the possibility of the U.S.S.R. acquiring the necessary cryptographic materials through Method 2.*

c. Any half hearted approach might prejudice a later approach based [redacted] furthermore, any approach by stages might lay the U.K. and the U.S. Governments open to French accusations of insincerity.

d. Acceptance by the French M.F.A. of participation by U.K./U.S. experts in the necessary drastic reorganization of its Cryptographic Service would not be likely to follow this approach.

e. The necessary number of cipher machines for this purpose is not available to meet French needs. Even if they were available, it could be anticipated that other NATO countries would make similar demands which could not be met.

*By obtaining physical possession of the cryptomaterial (key lists, code books, etc.) necessary for direct reading of the intercepted traffic.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~CONDITIONS GOVERNING AN APPROACH TO THE FRENCH

46. In order to induce the French M.F.A. to undertake the drastic overhaul required for real improvement in its communications security, any U.K. or U.S. approach should be calculated to shock the Ministry into making a major effort. It is considered that the only effective and practicable shock

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

47. Revelation [redacted] entails such grave risks that it should be subject to the conditions outlined below:

a. Prior to the initial approach there must be valid indications that the French M.F.A. and those other French Government Departments and Agencies which have access to M.F.A. communications containing information handled on a classified basis by the U.K. or the U.S. Governments have the intent and capability to establish arrangements to protect this information; these arrangements must be sufficient, in the agreed opinion of the U.K. and the U.S. Governments, to warrant making an initial approach.

b. The initial approach must be made at a point of contact in the French M.F.A., which contact is discreet, reliable, and at a level of sufficient authority. This contact should be informed:

(1) [redacted]

(2) [redacted]

(3) that, should he not believe this statement, a demonstration will be given to his experts provided he will give assurances that his Ministry will:

- (a) undertake an energetic program for reorganization of its Cryptographic Service and appropriate replacement of its present cryptographic systems and practices;
- (b) accept without qualification and promulgate U.K./U.S. essential standards of security in each phase and aspect of the program;
- (c) accept direct U.K./U.S. participation in executing the program, including participation on a working level by representatives qualified in the field of general security as well as all aspects of communications security.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET ACORN~~

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

TAB "B" CONTINUED

c. Should a [redacted]

be unnecessary to convince the contact as to the [redacted]

[redacted] nevertheless, before any further steps in the program are undertaken,

the assurances set forth in paragraph b(3) must still be obtained.

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

4B. In informing the French M.F.A. of details [redacted] of its

cryptographic systems, it is essential that as little information as possible
be divulged [redacted]

[redacted] These should be selected so as to reveal the minimum amount of

technical information, which should be restricted to the level of [redacted]

[redacted] systems. If any disclosure of [redacted] information relating to [redacted]

[redacted] should be found necessary in order to obtain French [redacted]

acceptance to the conditions specified in paragraph 47b, such disclosure will

not be made without prior agreement between the U.K. and the U.S. Governments.

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

~~TOP SECRET AGON~~~~TOP SECRET CANOE~~TAB "C"MEANS OF APPROACH

49. An initial approach to the M.F.A. at a level of sufficient authority offers a choice between the Minister and the Secretary-General. It is considered that the latter would be the more suitable point of initial approach for the following reasons:

a. The Secretary-General is a permanent official, while the Minister is liable to replacement;

b. As a Department official, the Secretary-General is more likely than the Minister to take a comprehensive and continuous view of the problem;

c. The outstanding personality and known reliability of the Secretary-General, M. Alexandre Parodi, are believed to be such as to offer good prospects of effective implementation of the U.K./U.S. plan.

50. All subsequent widening of the circle of discussion will require precise definition and prior U.K./U.S. agreement.

51. The various risks arising [redacted] particularly the [redacted] require that [redacted] but not both, the logical nominees being the U.K. [redacted] the French have been associated in the past.

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

52. There would be distinct advantages in a U.K./U.S. joint approach based on joint consultation and joint recommendations in the light of the [redacted] In view of the fact that a considerable effort on the part of the French is required, the maximum available pressure must be exerted.

53. Inasmuch as the U.K. and the U.S. Ambassadors in Paris have already been apprised of this problem and in view of their official positions, it is logical that they should make the initial approach to M. Parodi.

~~TOP SECRET CANOE~~