

REPORT
TO
THE LONDON SIGNAL INTELLIGENCE BOARD
AND
THE UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
ON
THE U.K. - U.S. CONFERENCE ON THE SECURITY OF FRENCH COMMUNICATIONS
HELD AT WASHINGTON, D.C., COMMENCING 1 MAY 1951

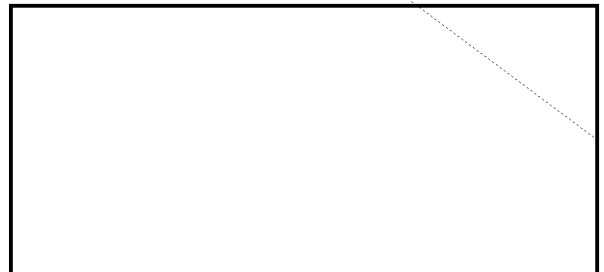
1. As the result of an LSIB proposal of 12 December 1950* and the USCIB acceptance thereof, communicated to LSIB by letter dated 19 January 1951,** a U.K. - U.S. Conference to consider the improvement of French communications was held at Washington commencing the 1st of May, 1951.

2. The detailed conclusions and recommendations of the Conference which are set forth in the accompanying report are submitted for approval by the London Signal Intelligence Board and the United States Communications Intelligence Board.

PL 86-36/50 USC 3605



EARL E. STONE
Rear Admiral, U.S. Navy
Chairman, U.S. Delegation



* SB/783
** UC #00015

~~TOP SECRET ACORN~~

REPORT

OF THE

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

HELD 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".

CONCLUSIONSEO 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 and 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 ACORN~~

~~TOP SECRET ACORN~~

[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", 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 ACORN~~

~~TOP SECRET ACORN~~

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 [redacted] collaboration.

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

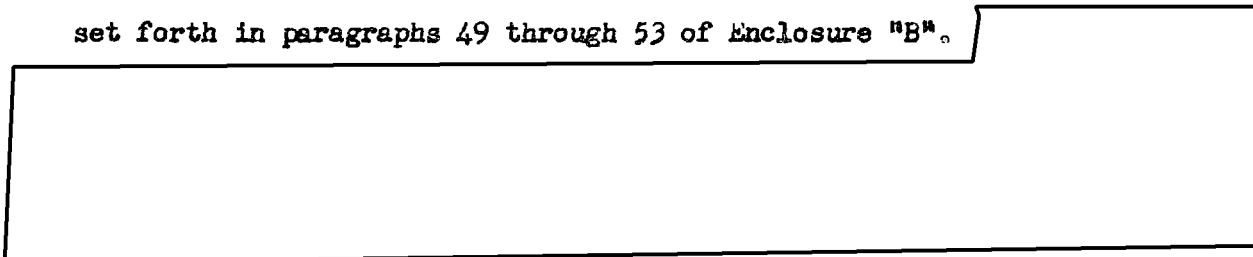
j. Provided the conditions set forth in paragraphs 46 through 48 of Enclosure "B" for minimizing these risks can be met, an approach to the French M.F.A. is warranted.

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 [redacted] 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".



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 earmarked for this purpose, the latter being phased in consonance with NATO needs.)

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

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 ACORN~~

~~TOP SECRET ACORN~~ENCLOSURE "A"PLAN FOR IMPROVING THE CRYPTOGRAPHIC SECURITY OF
FRENCH DIPLOMATIC COMMUNICATIONS

1. French diplomatic posts should be divided into three categories:

a. Category I: Posts which handle the most critical information and in considerable volume, such as Paris, London, and Washington.

b. Category II: Other posts whose communications include information which should have complete protection.

c. Category III: All other diplomatic posts.

Note: 32 of the posts which should be included in Categories I and II are listed in Paragraph 3 below.

2. The systems recommended for these three categories are: .

a. For Category I:

(1) The Combined Cipher Machine (CCM) with Simplex settings. The word Simplex is used to mean a procedure whereby each message has its own rotor arrangement and alignment provided by means of a special key list. The lists are prepared for point-to-point use so that a post can decipher only those messages specifically addressed to it. For the transmission of multiple-address messages, a multiple holder Simplex key list is also provided.

(2) A one-time pad system should be provided as an emergency stand-by in this category. The number of posts that will be included in Category I will be determined by the number of equipments that can be made available. It is not yet possible to ascertain the phased program for the supply of machines for this purpose primarily because of commitments already made to NATO. A small number of machines (approximately 20) can be supplied initially to cover the most important posts. As additional machines become available, further posts can be changed from Category II to Category I. The greater the number of posts which can be included in Category I, the more simple becomes the problem of multiple one-time pad networks for Category II.

b. For Category II: A numerical two-part code book with one-time pad.

~~TOP SECRET ACORN~~

It is recommended that new code books be prepared and issued for this purpose.

c. For Category III: Selected French diplomatic systems could continue in use, new two-part code books with frequent changes being recommended.

3. The principal posts to be included in Categories I and II are as follows:

Ankara	Cairo	Moscow	Saigon
Athens	Copenhagen	New Delhi	Singapore
Baden	Djakarta	New York	Stockholm
Bangkok	The Hague	Oslo	Taipei
Belgrade	Karachi	Paris	Teheran
Berlin	Lisbon	Rabat	Tokyo
Bonn	London	Rangoon	Vienna
Brussels	Madrid	Rome	Washington

4. The foregoing will provide the French Ministry of Foreign Affairs with secure systems but it is also necessary that technical assistance be provided to insure that the requirements of procedural and transmission security, which are also involved in communication security, will be met. Therefore, the U.K./U.S. Governments are prepared to furnish such assistance and to make available the services of qualified technicians to assist the French technicians on the working level.

~~TOP SECRET ACORN~~FACTS BEARING ON THE PROBLEM AND DISCUSSIONINDEX OF CONTENTS

	EO 3.3(h)(2) PL 86-36/50 USC 3605	<u>Paragraphs</u>	<u>Page</u>
GENERAL STATEMENT		1-3	8
CONSIDERATIONS AS TO FRENCH INTERNAL INSECURITY		4-11	8
PERSONNEL AND PHYSICAL SECURITY OF FRENCH CRYPTO- GRAPHIC SERVICES		12-16	10
FRENCH MILITARY COMMUNICATIONS		17-19	11
FRENCH DIPLOMATIC COMMUNICATIONS		20-24	11
APPROACH TO THE FRENCH 		25-26	13
TECHNICAL PLAN FOR IMPROVEMENT OF FRENCH DIPLOMATIC COMMUNICATIONS		27-35	14
ADVANTAGES AND DISADVANTAGES INHERENT IN THE U.K./U.S. PROPOSAL FOR THE IMPROVEMENT OF FRENCH DIPLOMATIC COMMUNICATIONS SECURITY		36-37	16
ASSESSMENT OF LIKELIHOOD AND EXTENT OF RISKS INVOLVED		38-45	18
CONDITIONS GOVERNING AN APPROACH TO THE FRENCH		46-48	19
MEANS OF APPROACH		49-53	21
NECESSITY FOR FURTHER STUDY		54-57	22

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~ENCLOSURE "B"FACTS BEARING ON THE PROBLEM AND DISCUSSIONGENERAL STATEMENT

1. Intelligence may be derived from cryptocommunications by any or all of the following methods:

a. By obtaining physical possession of the exact texts or the substance of the communications (hereafter called Method 1);

b. By obtaining physical possession of the cryptomaterial (Key-lists, code books, etc.) necessary for direct reading of the intercepted traffic (hereafter called Method 2);

c. By interception and cryptanalysis of the communications (hereafter called Method 3).

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


2. With respect to intelligence derivable from present French communications, the U.S.S.R. is in a position to employ all three methods,



3. The U.K. and the U.S. Governments have the technical knowledge required for improving the security of French diplomatic communications to a degree sufficient and necessary to deny Method 3 to the U.S.S.R. They also have knowledge of security practices which, if enforced, would provide reasonable assurance of denying Methods 1 and 2 to the U.S.S.R. However, the denial of Methods 1 and 2 will depend ultimately upon physical security as well as the reliability and discretion of those who are responsible for handling and safeguarding classified information in the French Government, and especially in the Cryptographic Service of the French Ministry of Foreign Affairs (M.F.A.)

CONSIDERATIONS AS TO FRENCH INTERNAL INSECURITY

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

 a number of French Government Departments and Agencies are at present, and to varying degrees, infiltrated with French Communists and other disloyal or untrustworthy personnel. Although there is no positive evidence of extensive penetration by U.S.S.R. agents, the U.K. and the U.S. Governments cannot

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

afford to disregard this probability.

5. Although neither the U.K. nor the U.S. Government has positive evidence that French Communists or U.S.S.R. agents in French Government offices have passed classified information in volume to the U.S.S.R., the assumption that it occurs not only sporadically but continuously also cannot be disregarded.

6. [REDACTED] violent internal dissensions, personal, departmental and inter-departmental feuds within and among some French Government Departments and Agencies have led to the disclosure of classified information.

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

7. [REDACTED] although the French Government has regulations for the protection of classified information, these are not enforced and that in at least some French Government Departments and Agencies there has been gross carelessness in the storage and handling of classified documents.

8. A Tripartite Group (U.K., U.S., and French) is now surveying and studying the internal security of the French Government, especially in regard to the nature and adequacy of French regulations and facilities for the protection of classified information.

9. Some improvements in French internal security have been made recently and to a certain degree disloyal elements have been eliminated. Further improvements in internal security may be expected as a result of the work of the Tripartite Group.

10. Available evidence suggests that insecurity prevails in French Departments and Agencies as indicated below:

a. Air Ministry. This Ministry is a particularly bad offender, both as regards penetration and lack of discipline in the application of security procedures.

b. Armed Forces. In the Army and the Air Force, probably less than 5 percent of the officers are Communists, but the percentage in the ranks is considerably higher, possibly 15-20 percent. In the Navy, these percentages are considerably less.

~~TOP SECRET ACORN~~

c. P.T.T. (Posts and Telegraphs). This administration is seriously penetrated by Communists.

d. The S.D.E.C.E. (French Secret Service) and the Surete do not meet the security requirements of high-grade intelligence and security services.

e. Instances of insecurity have been found in the Ministries of Defense, Armaments, Industrial Production and Labor, in the Atomic Energy Commission, and in various nationalized industries.

11. As regards the French M.F.A., the Ministry particularly concerned in this report, there is little verifiable evidence of insecurity, although there are grounds for suspicion; nevertheless a certain proportion of plain-language texts of French diplomatic telegrams is no doubt circulated among other Departments and Agencies known to be insecure.

PERSONNEL AND PHYSICAL SECURITY OF FRENCH CRYPTOGRAPHIC SERVICES

12. Disloyalty on the part of cryptographic personnel or penetration by enemy agents into cryptographic offices is recognized as the greatest hazard to the security of cryptographic communications and the one most difficult to eliminate. The U.K. and the U.S. Governments have found that special procedures are necessary to combat this hazard and have established special provisions for the physical security of the premises on which cryptographic activities are conducted.

13. Neither the U.K. nor the U.S. Government has information concerning the physical security procedures of the French cryptographic services or the methods employed for screening their personnel.

14. Neither the U.K. nor the U.S. Government has direct evidence of Communist penetration of the French cryptographic services, but in view of the general conditions described in paragraphs 4 through 11, they must assume that such penetration exists here also. (There is some evidence to indicate insecurity arising from carelessness of individual members of these services and inadequate physical security.)

15. There can be no assurance that the U.S.S.R. would be denied intelligence by means of Methods 1 and 2 until personnel and physical security in the French cryptographic services attain standards acceptable to the U.K. and the U.S. Governments.

16. The foregoing considerations are applicable to the Cryptographic Service of the French M.F.A. and are therefore of particular concern in this report.

FRENCH MILITARY COMMUNICATIONS

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

17. The U.K. and U.S. authorities, having agreed upon the desirability of improving NATO communications, have offered to provide, inter alia, the Combined Cipher Machine (CCM) for NATO communications, an offer already accepted by the French. It should be noted that this is being done through the multi-lateral mechanism of NATO

[Redacted]

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

[Redacted]

It is felt that this aspect of insecurity in French military communications can be corrected, however, [Redacted] i.e., indirectly, through the precedent established in providing the CCM as the military cipher machine for NATO communications.

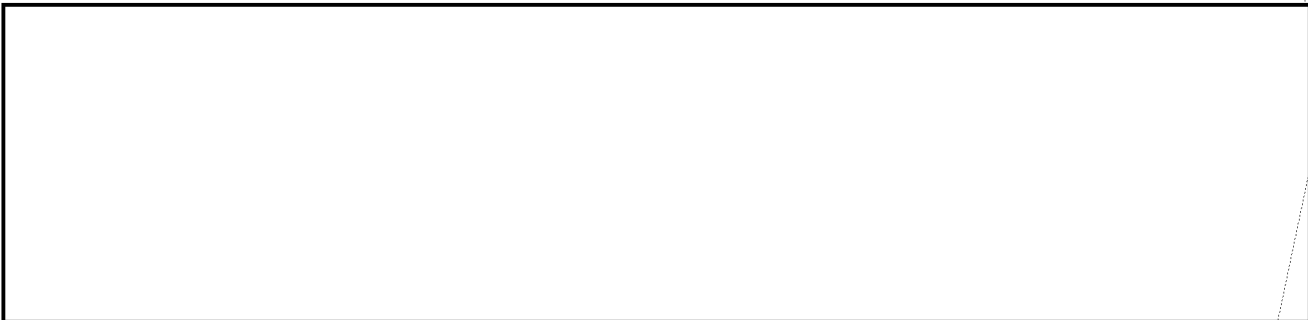
EO 3.3(h)(2)
PL 86-36/50 USC 3605

19. In view of the foregoing, and because it is considered that the primary source of present loss of important intelligence through insecure communications is in the diplomatic and NATO spheres, the remainder of this Enclosure is devoted exclusively to the situation as regards French diplomatic communications.

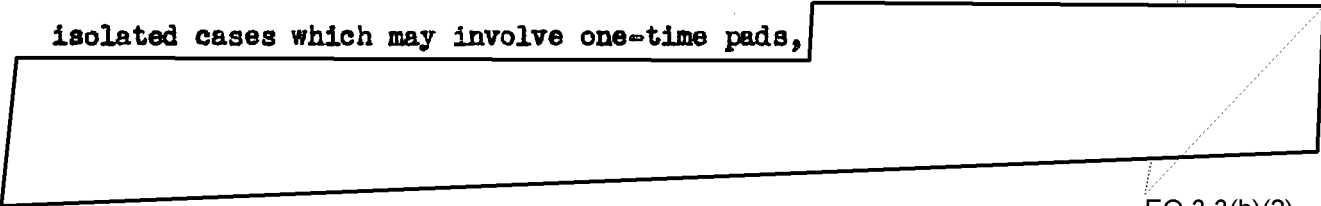
EO 3.3(h)(2)
PL 86-36/50 USC 3605

FRENCH DIPLOMATIC COMMUNICATIONS

[Redacted]



22. In regard to the current French diplomatic communications, observed French practices in cryptographic system design and distribution provide direct evidence that the present cryptographic organization 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. Except as regards one machine system of limited application referred to in paragraph 33, and with the further exception of certain isolated cases which may involve one-time pads,



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

~~TOP SECRET ACORN~~

23. Although a tradition of sound communication security doctrine did exist in France, the current cryptographic practices observed in French diplomatic traffic indicate that the French have fallen far behind the U.K. and the U.S. in matters pertaining to communication security. Therefore, technical assistance from outside the Cryptographic Service of the French M.F.A. is deemed essential for the success of any communication security program.

24. Satisfactory improvement in the security of the communications of the French M.F.A. will necessitate a drastic and expensive reorganization of its Cryptographic Service and that:

- a. The current cryptographic systems of the M.F.A. be replaced with secure systems for use in all important posts;
- b. Technically sound communication security procedures be established;
- c. Adequate training in the use of the new systems and procedures be assured;
- d. Careful technical supervision be exercised by the French over their diplomatic communications in order to maintain communication security.

APPROACH 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

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

~~TOP SECRET ACORN~~

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.

TECHNICAL PLAN FOR IMPROVEMENT OF FRENCH DIPLOMATIC COMMUNICATIONS

27. Enclosure "A" presents a plan for improving the security of French diplomatic communications.

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

28. This plan has been drawn up with two main objects in view: first, to insure that there should

[redacted] to provide the maximum protection against the effects of partial U.S.S.R. penetration by Methods 1 and 2.

29. The CCM has obvious operational advantages as compared with existing slower and more laborious hand systems. For the transmission of international diplomatic or highest-level military traffic dealing with NATO affairs, the French have been provided with TYPEX machines and they are presently using a Simplex procedure with these machines in the highest echelons of NATO; the CCM is also being offered to them, as well as to other NATO signatories, for NATO communications and has already been accepted by the French. Adequate training in the new systems will therefore be simplified as a result of previous experience.

30. The localization introduced by using Simplex procedures with the CCM has a double advantage. First, it increases cryptosecurity generally (an operating error will involve at most the compromise of one message as opposed to that of all the traffic sent in one day on a particular channel); secondly, if there should be an instance of penetration by the U.S.S.R. at any cryptographic installation other than the central Paris offices, the

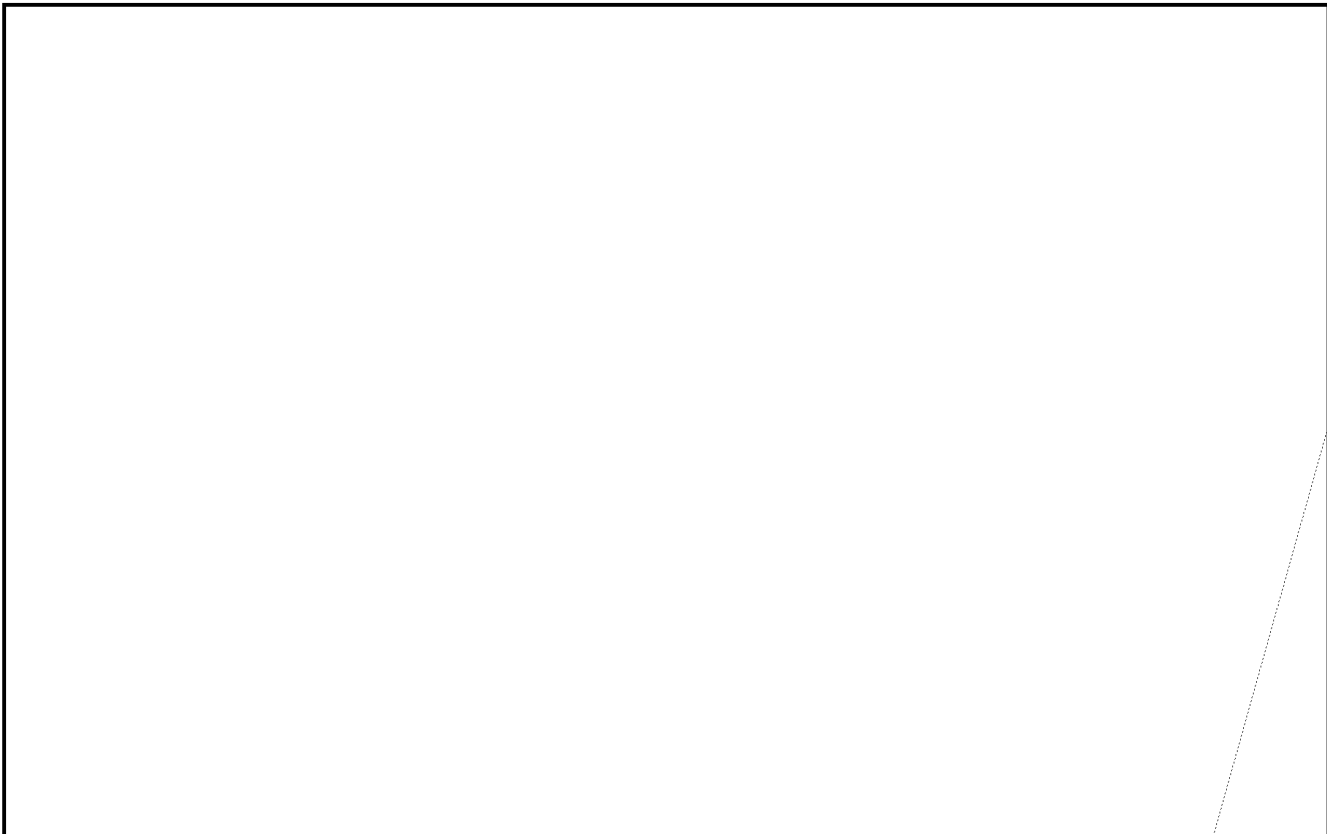
dangers resulting from such penetration would be confined to those cryptonets in which that installation is involved.

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

31. The plan in Enclosure "A" proposes for a level of communications designated as Category II a numerical two-part code book with one-time pad. The advantages pointed out in paragraph 30 apply equally to the one-time pad cryptonets. Considerable experience on the part of the British (and particularly of their Foreign Office) in the field of one-time pad usage has shown the implementation of complex one-time pad networks to be entirely practicable.



32. There will be an important and major requirement to instruct the French M.F.A. in the large-scale production of one-time pads. It is not improbable that the M.F.A. is very little versed in these uses of IBM/Hollerith machinery and has at present very little, if any, of the equipment available. Adequate detailed technical instruction can nevertheless be given to the French technicians without disclosing cryptanalytic information.



34. It is not felt that other machine systems available elsewhere in the French Government would be proposed or adopted for use by the French M.F.A. (despite the fact that the Modified B-211, for example, may equal the CCM in operational efficiency), due to the limited supply available and the cost

of new machines which would have to be manufactured. In addition, the adoption of the CCM would follow a pattern already started for top-level NATO diplomatic communications and thereby provide greater uniformity and simplicity of organization.

35. Owing to the limited U.K./U.S. stock of CCMs and to the fact that undertakings already made in respect to NATO requirements for this machine cannot be met from existing stocks but call for new production, it is necessary to devise a phased program for the allocation of CCMs to the French M.F.A. It is considered that ultimately a total of 80 equipments should be earmarked for this purpose but in the light of the above an initial immediate issue of about 20 equipments should be made. Of these, the U.K. can provide approximately 8, the U.S., 12 machines. The extent to which the issue of the remainder should be phased in relation to the NATO plan must be a matter for discussion and agreement between the U.K. and the U.S. Governments.

ADVANTAGES AND DISADVANTAGES INHERENT IN THE U.K./U.S.
PROPOSAL FOR THE IMPROVEMENT OF FRENCH DIPLOMATIC
COMMUNICATIONS SECURITY

36. If the U.K./U.S. plan for improving French diplomatic communications security is successful, then, subject to the conditions noted in paragraphs 46 through 53 below, the following advantages would result:

a. Assuming that the U.S.S.R. is reading a significant proportion of the French diplomatic traffic, the U.S.S.R. would be denied (1) its speediest, most reliable, and, possibly, its most prolific source of information on French foreign policy; (2) a speedy and reliable source of information on Western policy in all matters calling for effective French participation; and (3) a valuable source on conditions in countries other than France, as reflected in French diplomatic traffic.

b. Denial to the U.S.S.R. of information from COMINT sources would be seriously detrimental to the efficiency of U.S.S.R. intelligence organizations and thereby diminish the value of information derived from penetration by means of agents. (The U.K. and the U.S. members agree that an extensive and continuous flow of communications intelligence is a more rapid and a more reliable source of information than are the covert operations of any organization of agents; it is largely prerequisite to optimum intelligence operations.)

c. Both U.K. and U.S. Governments and individual officials would be able to negotiate more freely in direct dealings with the French.

d. Steps taken to improve the security of communications of the French M.F.A. may pave the way and assist in steps to improve the over-all internal security of the French Government, and, since that Government is one of the more important members of NATO, will improve the security of NATO as a whole.

37. The following are disadvantages either inherent in or possible results of the proposed approach to the French M.F.A.:

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



c. Political disadvantages through [redacted] collaboration. It would appear that the political impact of the disadvantage described in 37b(2) above would be greatly increased if such a [redacted]

[redacted] activity. It would become obvious that despite the evident political differences between the U.K. and the U.S. Governments, they have been able to collaborate effectively in the present instance in a field where national secrets are given the highest safeguards.

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

d. The creation of a false sense of security on the part of U.K. and U.S. officials. The removal of evidence of insecurity in French diplomatic communications may, [redacted]

[redacted] lead to the unwarranted assumption that

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

other French security weaknesses have also been corrected.

ASSESSMENT OF LIKELIHOOD AND EXTENT OF RISKS INVOLVED

38. Despite the possibility that political instability in the French Government may affect the permanence or continuity of remedial measures which may now be applied to French insecurity, it is not felt that this consideration applies so directly to this problem as to preclude an approach to the French M.F.A.

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

39. The disclosure of [redacted]

[redacted] may generate pressure from the French for [redacted]

[redacted] is suggested by the French as a con-

dition for their acceptance of extensive U.K./U.S. intrusion in their cryptographic affairs, this suggestion must be firmly rejected. It is not considered that this problem presents a major obstacle.

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

40. Even if all three methods of obtaining intelligence from French diplomatic communications were largely denied to the U.S.S.R., it is considered that, [redacted]

[redacted] This risk is not inherent in the U.K./U.S. technical plan for improvement of French diplomatic communication security, but lies rather in the possibility that the French will be unable to safeguard effectively the [redacted]

[redacted] It is felt that an approach can be devised which will provide some assurance in this regard. (The development of the cryptography of most of the countries concerned has not in fact indicated that they always respond effectively to such revelations.)

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

[redacted]

42. It must be emphasized that the advantages enumerated in paragraph 36 are largely contingent upon sufficient improvement in French internal security to deny the U.S.S.R. intelligence derived from Methods 1 and 2. If a U.K./U.S. plan for improving the security of French diplomatic communications is adopted and made effective, thus denying Method 3 to the U.S.S.R.

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

without eliminating Method 2, then the U.S.S.R. will still have the benefit of the Methods 1 and 2. If both Methods 2 and 3 were denied the U.S.S.R. there would still be a significant direct leakage of intelligence to the U.S.S.R. through the Soviet intelligence organization and French Communist Party channels.

[REDACTED]

43. Referring to the disadvantages noted in paragraph 37c, it is felt that these political disadvantages are outweighed by the gains to be derived if the improvement in the security of communications of the French M.F.A. is effective.

44. Referring to the disadvantage noted in paragraph 37d, avoidance of the false sense of security mentioned therein is a problem the solution of which lies within our own control.

45. It is felt, therefore, that, by recognizing certain conditions and establishing specific means of obtaining satisfactory assurances with regard to them, the likelihood and extent of the risks involved can be so reduced as to realize a sufficient gain and warrant an approach to the French M.F.A. The paragraphs which follow deal with these conditions and means.

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 would be the

[REDACTED]

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

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

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.

~~TOP SECRET ACORN~~

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:



(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:

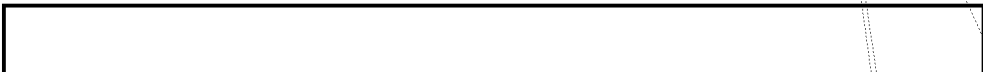
(a) undertake an energetic program for reorganization of its Cryptographic Service and appropriate replacement of its present cryptographic systems and practices;

(b) accept without qualification and promulgate U.K./U.S. essential standards of security in each phase and aspect of the program;

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

(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.

c. Should a



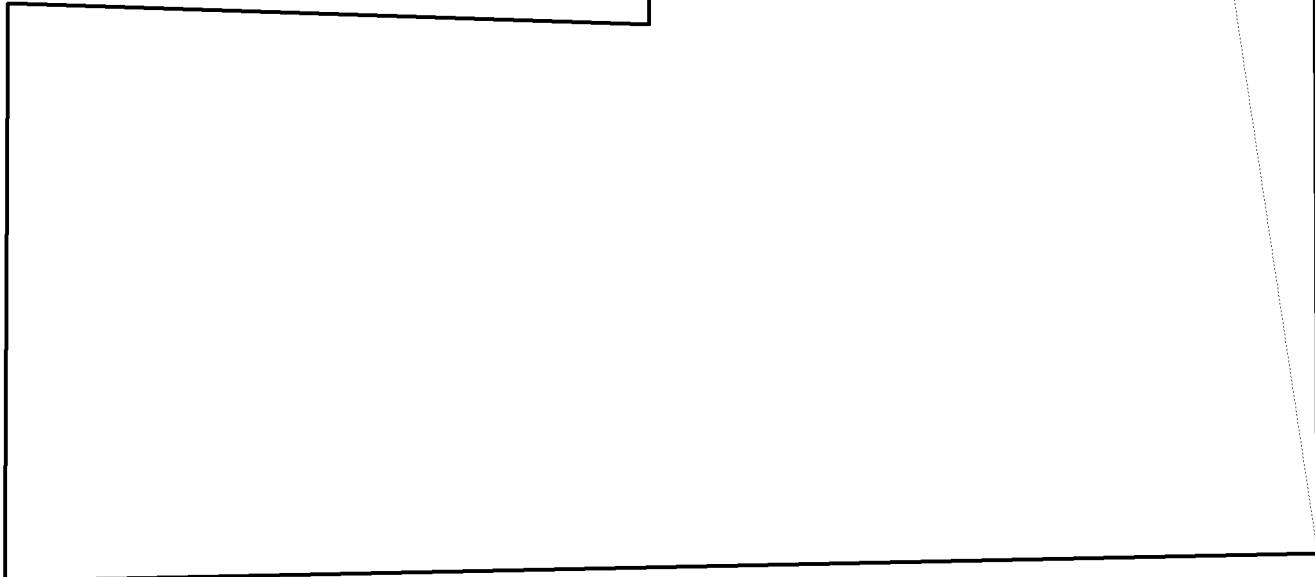
be unnecessary to convince the contact as to the



nevertheless, before any further steps in the program are under-

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

48. In informing the French M.F.A.



~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

[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] systems. If any disclosure of [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 3605MEANS 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. with whose [redacted] the French have been associated in the past.

EO 3.3(h)(2)
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.

~~TOP SECRET ACORN~~

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.

NECESSITY FOR FURTHER STUDY

54. In view of the fact that certain of the conditions to be met by the French Government prior to the approach to the French M.F.A. are not yet satisfied, and in order to exercise some supervision over the implementation of the plan for improving the security of French diplomatic communications, it is desirable that LSIB and USCIB keep the problem under continuous review.

55. When the U.K. and U.S. Ambassadors make their initial contact with the French M.F.A., it would be advisable that the respective Chairmen and/or nominees visit Paris to brief their Ambassadors, and also to participate as required.

56. Since it is impossible to foresee all contingencies in making the approach and in implementing the cryptographic plan, it is advisable that LSIB and USCIB be authorized to take such additional implementing action as they may agree.

57. When LSIB and USCIB agree that the requisite security conditions have been met, it is advisable that the approach be initiated without further authorization.