

USCIB: 23/30

8 October 1951

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Portuguese Communications Security.

1. Pursuant to USCIB decision at the 68th Meeting, the attached detailed report has been prepared by CIA and Department of State representatives.

2. This report will be considered in connection with item 3 of the agenda for the 70th USCIB Meeting.

H. G. Jones
H. G. JONES
J. W. PEARSON
Secretariat, USCIB

Inclosure 1 Dept. of State memo dated 4 Oct. 1951.

USCIB: 23/30

Declassified and approved for release by NSA on 07-16-2014 pursuant to E.O. 13526

DEPARTMENT OF STATE
WASHINGTON

4 October 1951

MEMORANDUM FOR THE CHAIRMAN, USCIB

SUBJECT: Portuguese Communications Security

1. At its Sixty-eighth Meeting on 10 August 1951, USCIB decided that the Department of State and the CIA should prepare jointly a detailed plan for a direct approach to the Portuguese Government based on the proposal contained in paragraphs 11 and 12 of the Ad Hoc Committee Report to USCIB on this subject (USCIB 23/22 dated 7 August 1951). The detailed plan which has been prepared and approved by the Department and CIA is presented in the paragraphs which follow in terms of its objectives, bases, the means available and the procedures to be followed.

2. Objectives of the plan.

- a. To obtain assurances that Portuguese representatives in NATO will observe requests of US representatives regarding the handling of classified information made available by the United States;
- b. To reduce the leakage of COSMIC and NATO TOP SECRET and SECRET information through the insecurity of Portuguese Communications; and
- c. To induce the Portuguese Government to make more use of the authorized NATO cryptographic system (TYPEA) and to compile their own books of cryptographic settings for use in connection with the TYPEA.

3. Bases for the plan. The approach must demonstrate that:

- a. The security of highly classified US information and plans has been jeopardized through mishandling by the Portuguese;
- b. COSMIC information has been involved;
- c. The mishandling has included (1) disregard of the request of a US representative making the information available and (2) violation of NATO security practices;

Inclosure with USCIB 23/30 dated 8 October 1951.

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

d. The US has received indications that the Portuguese do not consider TYPEX a reliable cryptographic system; and

e. The US considers TYPEX to be entirely suitable and that its reliability can be demonstrated by appropriate US or NATO officials.

4. Means available.

a. Direct access by the US Ambassador in Lisbon to the Premier of Portugal.



c. [redacted] obtained from a source in western Europe who had in turn obtained the information from a contact through whom he had had brief access to a copy of the cable from Ulrich to his Government. The source and his original contact are not identified specifically in order to



of which the US Government has direct knowledge.

5. Procedures.

a. The matter is to be handled personally and exclusively between Ambassador MacVeagh and Premier Salazar and is to be known only to the Ambassador among US Embassy personnel in Lisbon.

b. Ambassador MacVeagh is to receive his instruction in this matter in Washington.



d. If considered suitable by Ambassador MacVeagh, his approach to Premier Salazar is to be made along the following lines:

- (1) Establish the delicacy and urgency of this problem to the US Government.
- (2) Present the evidence pointing out that the original source and his reliability are not known, but that most of the information contained in the report is known to be true by the US Government, and that it must be assumed, therefore, that those facts contained in the report to which the US Government is not directly privy may also be correct. *Statements*
- (3) Point out that, if this assumption is correct, the US is greatly concerned over: (a) the leakage of critical US classified information; (b) Ulrich's apparent disregard of the specific request for special handling of the information contained in para g of the report; and (c) the apparent Portuguese disregard for the authorized NATO cryptographic system.
- (4) Require categorical assurance from the Portuguese Government that (a) its representatives would observe the requests of US representatives regarding the handling of classified information made available by them and that (b) NATO security practices, including the use of the authorized NATO cryptographic system, would be observed at all times.
- (5) Offer the assurances of US Government that the TYPIA is a reliable cryptographic system and that its use as required by NATO security regulations is a necessary security precaution; pointing out that, if the Portuguese require further assurance of this, they might request a demonstration of the security features of the machine from either the US Government or the Security Coordinating Committee of the NATO Standing Group.

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



6. A copy of the [redacted] to be used in this approach is attached hereto as Enclosure 1. It consists of a translated extract from [redacted]

7. Ambassador MacVeagh is expected to arrive in Washington for consultation on or about 5 October. In order that this matter may be taken up with him while he is here, it is requested that USCIB consider this plan at its meeting on 12 October and that the views and concurrence of the British in the general approach have been obtained by that time.

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

/s/ W. Park Armstrong, Jr.
W. PARK ARMSTRONG, JR.
Special Assistant, Intelligence

Enclosure

[redacted]

(EXTRACT - TRANSLATION)

A usually reliable source, with excellent contacts in western European diplomatic circles, has provided the information set forth below without, however, identifying the contact from whom he obtained the report.

1. Rui Ulrich, the Portuguese Ambassador to London, recently cabled a report to his Government covering a recent meeting of NATO representatives in London. The salient points were as follows:

- a. The discussion at the meeting centered around the question of the admission of Greece and Turkey to the Atlantic Pact organization.
- b. Several members of the NATO group, notably the Scandinavians, opposed the inclusion of Greece and Turkey into the NATO and proposed that a Mediterranean Pact be established which would be composed of the major powers, and to which Greece and Turkey would be invited.
- c. The president of the meeting did not agree with this proposal, indicating that a Mediterranean Pact would merely cause duplication of the NATO organization and would cause unnecessary complications in political and military situations.
- d. The president added that the incorporation of Greece and Turkey into the Atlantic Pact would not necessarily be cause for war, but might increase political and economic pressures on Greece and Turkey.
- e. Regarding air bases, the president expected that Turkey would make facilities available as had the other NATO countries, but stated that the United States would admit Turkey to NATO even with limited use of airfields. Ulrich reported that this information was so sensitive that the representatives were asked not to telegraph it to their governments, a precaution which he personally felt was not necessary.
- a. f. Ulrich concluded by advising that the Pact machine (sic) was not sufficiently secure for sensitive information.

Field Comment. Source states that the lack of specific details in the report should be attributed not only to the fact that the information was received second-hand, but to the extremely short period of time the information was made available to him by his contact.

Washington Comment. It has been determined that the discussion reported above took place at the 5th of July, 1951, meeting of the NATO Council Deputies.

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

REPORT BY THE USCIB AD HOC COMMITTEE

to the

UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

ON

PORTUGUESE COMMUNICATION SECURITY

Reference: USCIB: 23/18

1. At its 66th Meeting, 13 July 1951, USCIB approved the referenced Report, which recommended that:

"b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government."

2. The Ad Hoc Committee has continued its study of the problem, and has developed the additional facts and conclusions set forth below.

3. The NATO security system and regulations designed to protect sensitive NATO information are adequate for the purpose*. The definitions "COSMIC" and "NATO" information are clear and susceptible of being applied with precision.

*It is anticipated that a new document, D.C. 2/7, which was approved by the Standing Group and the Military Representatives Committee of NATO on 13 April 1951, and which is now awaiting final approval by the Council Deputies, will soon become effective. The new document will merely amplify and, in small measure, clarify the current security system and regulations.

4. Some Portuguese communications which contain information that clearly falls within the limits stipulated by the definitions are secure, since these communications are being transmitted by the authorized cryptosystems, viz., TYPEX with simplex settings. However, even in cases where the Portuguese have used TYPEX, their lack of "know-how" in the communication security (COMSEC) field and the manner in which they use the machine make those messages possibly vulnerable to cryptanalytic attack and weaken the NATO TYPEX system as a whole.

5. Some NATO communications, however, contain information which may be characterized by the designation "NATO fringe traffic", and which consists largely of national comment on "COSMIC" or "NATO" matters and documents. At the time that the definitions of COSMIC and NATO information were elaborated, the question whether national comment was to be considered COSMIC or NATO information was discussed and specific provision that it be so considered was excluded. This exclusion was at the request of the Department of State, which, inter alia, did not wish its own representatives to NATO hampered in regard to this matter. In the case of Portuguese communications, it is both COSMIC or NATO material and this "fringe traffic" which constitute the principal sources of insecurity of NATO and U.S. information.

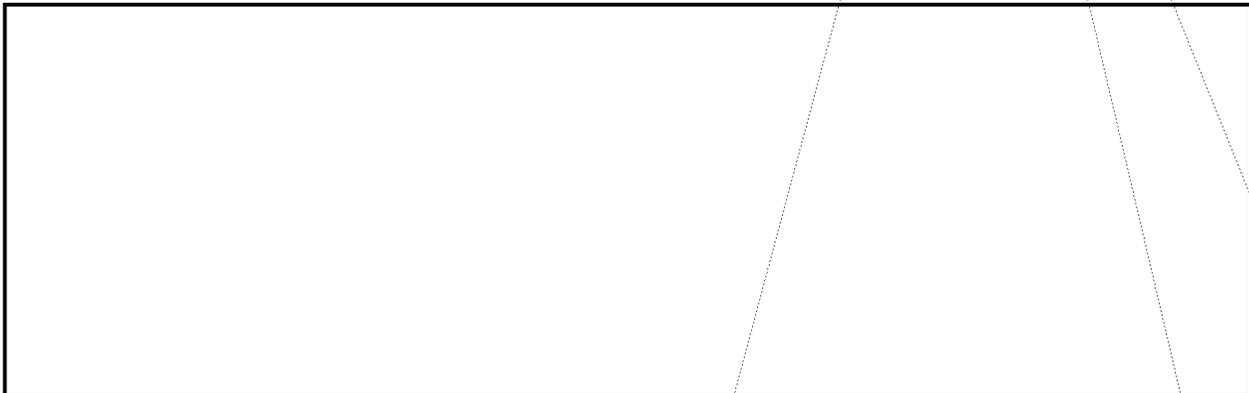
6. In transmitting national comment, the Portuguese member of the Council Deputies in London prefers to use a Portuguese cryptosystem rather than TYPEX because he fears that the British might read TYPEX messages, since the settings are provided by the British. The Portuguese cryptosystems used for this purpose is the Hagelin C-38 machine with such poor procedures that in all probability the U.S.S.R. and other countries are reading these Portuguese messages, even though they may be transmitted by wire systems.

7. On 25 April 1951 all NATO member nations were informed by SGM-616-51 that the Signatory Nations of the North Atlantic Treaty Organization were authorized, in addition to constructing their own

plugboard setting keys, to prepare individual national Books of Settings for TYPEX, should this be desired, "in order still further to preserve the discreet nature of the channels provided for National use." They were also informed at the same time that "the U.K. have prepared a memorandum describing a secure method for the compilation of simplex settings and a copy will be made available to other member nations if desired." The transmission of national content by TYPEX machines with national settings is not prohibited.

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

8. The Ad Hoc Committee has ascertained that not a single one of the NATO countries has yet availed itself of the opportunity to compile or to use its own National Books of Settings*, or even of the authority granted to construct its own national plugboard settings. There are, in the case of Portugal, no indications of an intention to do so in the near future.



10. The Ad Hoc Committee considered a number of proposals for action which might be undertaken to correct this situation. Preliminary to its deliberations the Committee agreed that the protection of  interests is still the overriding factor in this case, and that any solution which would definitely prejudice them should be undertaken only as a last resort. Of seven proposals worthy of serious consideration it attentively studied three which while appearing to offer the best chance of producing immediate or, at least prompt, remedial results, at the

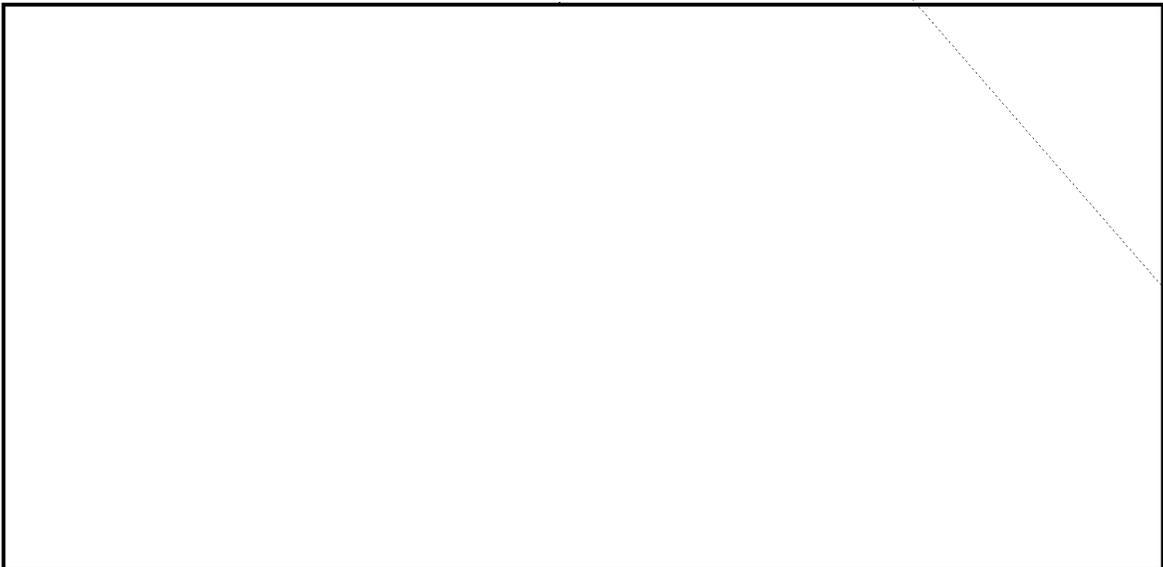
* Since the last meeting of the Ad Hoc Committee information has arrived indicating that as of 1 August Belgium has reported national settings for TYPEX but without recourse to the basic British instructional memorandum.



same time would present the least danger or security risk to the U.S.; the Committee then unanimously selected from among the three the one which it deems the most feasible and best under the circumstances. The details of the proposal thus selected are described in paragraphs 11 and 12 below; all proposals are set forth in Enclosure "A", together with comments.

11. The proposal finally selected by the Ad Hoc Committee is based upon these three premises:

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



c. A prompt amelioration of the present insecure situation can be expected if the Portuguese could be:

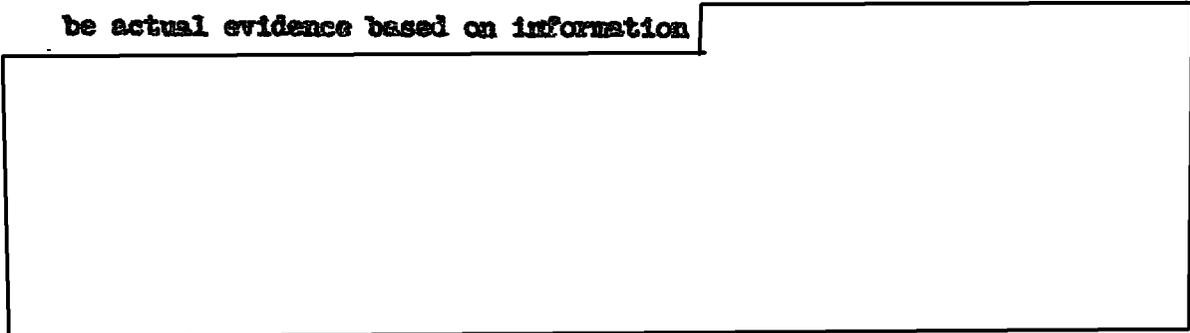
- (1) Forces to comply with NATO security regulations;
- (2) Given further indoctrination so that they would acquire full confidence in the security of TYPEX;
- (3) Induced to make more use of the NATO authorized cryptosystem (TYPEX); and
- (4) Persuaded to take advantage of the permission granted NATO members to compile their own national books of settings for TYPEX.

12. a. The selected proposal, based upon these premises, involves a direct, and apparently (to the Portuguese) unilateral (U.S.) approach on a Government-to-Government level, with a view to delivering a shock to the Portuguese Government by showing that:

- (1) Its representation on the Council Deputies is deliberately violating not only a well-defined NATO communication security regulation to which the Portuguese Government solemnly subscribed, but also manifests little hesitancy in disregarding an expressly stated request by the President of the Council Deputies that certain information be transmitted only by courier; and
- (2) The security violation involved the disclosure of highly sensitive U.S information of a character clearly political and of highest importance to NATO and U.S. Security.

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

b. The means or vehicle to be employed for this purpose would be actual evidence based on information



c. The Portuguese Government would be informed that the U.S. Government is so incensed and concerned about this flagrant violation directly affecting its own security, as well as that of the whole of NATO, that it considered referring the matter to the Council Deputies. Nevertheless it was reluctant to take such action, provided that prompt steps would be taken to correct the situation and that assurances would be given by the Portuguese Government that the action it will take will prevent a repetition of such violation and disregard of security procedures in future.

c. These assurances must comprise:

- (1) Assurance that a request by a member government presenting information to a NATO body that such information be transmitted only by accompanied bag will be strictly observed; and
- (2) Assurance that, when electrical transmission must be employed, only the authorized NATO cryptosystem (TYPEX)

will be used for the transmission of NATO information, as provided in NATO security regulations.

e. The approach thus far would not go beyond the point of taking care of the security of COSMIC and NATO TOP SECRET and SECRET information [the object of point (1) of paragraph 11c]; it would not take care of leakage from national comment on NATO matters [redacted] [the object of points (2), (3), and (4) of paragraph 11c]. Therefore, the approach should go further and attempt to give the Portuguese authorities positive assurance that the TYPEX is a secure means of communication, but [redacted]

This could be done by pointing

out that:

- (1) Unless some control were placed on the cryptosystems employed for the transmission of NATO information, identical or quite similar matter might be transmitted in as many as 12 different systems; and
- (2) A single cryptosystem, viz., TYPEX, was selected by the NATO Council after due deliberation because of the high degree of security it affords when properly used.

Should doubt remain, it could be suggested that the matter be referred to the Standing Group.

13. The Ad Hoc Committee is unanimous in its opinion that this proposal should be adopted, for the following reasons:

a. It appears to offer the only program for prompt remedial action which affords both security and a reasonable prospect of being effective. It is recognized that, to be effective, any approach to the Portuguese on this subject must shock them. This "shock" must be of such a nature that it will insure their compliance with NATO security regulations governing the transmission of classified NATO information, [redacted]

The use of the foregoing approach and the choice of [redacted]

[redacted] will produce this "shock", since this

[redacted] contains these important elements: (1) a violation of a specific request by the President of the Council Deputies not to transmit the information except by courier; (2) a statement clearly indicating that the Portuguese representative arrogates to himself the capability of reversing a judgment of the President of the Council Deputies as to the necessity for secrecy; and (3) a statement revealing the Portuguese attitude on the use of TYPEX.

b. It should be noted that the only currently available and positive evidence that the Portuguese are violating NATO security regulations and that their communications constitute a grave risk to the security of the U.S. and NATO has been [redacted]

c. It also provides an excellent opportunity to indoctrinate the Portuguese at the highest level in the actual security of the TYPEX system; it can be conducive to getting the Portuguese to use it for COSMIC, NATO TOP SECRET and SECRET information; and it may lead them to compile their own TYPEX settings for transmitting national content involving such information.

14. It will be necessary to obtain the concurrence of the London Signal Intelligence Board (LSIB) to this proposal, which should be communicated to that Board without delay if it is accepted by USCIB. A draft of a suitable memorandum to LSIB is contained in Enclosure "C".

15. a. The Ad Hoc Committee is of the opinion that the approach to the Portuguese outlined in paragraph 12 can be undertaken without referring the matter to the National Security Council (NSC) and without

awaiting the NSC decision on USCIB: 14/132 [redacted], since the proposed action does not involve [redacted]

b. The Committee also feels that the exact details of making the approach, the specific U.S. official or officials to be designated to make it, and the specific Portuguese official or officials to be approached, should be decided by the Department of State. A draft of a suitable memorandum to the Secretary of State is set forth in Enclosure "D".

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

16. The Ad Hoc Committee considers that:

a. All the other proposals set forth in Enclosure "A", except Proposal B [redacted] are suitable only as long-term programs;

b. It would be advisable to initiate action on one or more of those proposals as promptly as practicable so as to assure and extend the benefits which may flow from the Ad Hoc Committee's selected proposal for immediate action, as outlined in paragraph 12, if that proposal is approved and executed; and

c. Such long-term action may also lay the groundwork for Proposal B should it become necessary to resort to that proposal.

17. The Ad Hoc Committee further considers that Proposals A, D, E, and G, which are outlined in Enclosure "A", do not fall strictly within the cognizance of USCIB, although they are of interest to USCIB; that they should be studied in detail by the proper [redacted] security authorities of the Departments of State and Defense; and that they should be referred to these authorities by the State and Army members of USCIB. It may be noted that several of the long-term proposals are interdependent in the sense that they would reinforce one another and would be most effective if undertaken together under the same authorities.

18. Finally, with reference to the directive given the Ad Hoc Committee in USCIB: 23/18 to explore the possibility of instituting

safeguards involving greater use of courier service and of bringing this about through an approach to the Supreme Allied Commander Europe (SACEUR), the Ad Hoc Committee wishes to point out that the present Portuguese insecurity involves communications which are on the diplomatic level and not between military personnel. For this reason the matter is one in which SACEUR has no jurisdiction.

RECOMMENDATIONS

19. It is recommended that:

a. The action proposed in Paragraph 12, and Enclosures "C" and "D" be approved;

b. The long-term proposals outlined in Enclosure "A" be accepted in principle, for reference to the security authorities of the Departments of State and Defense.

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

ENCLOSURE "A"

PROPOSALS STUDIED BY THE AD HOC COMMITTEE
TO CORRECT THE
INSECURITY OF PORTUGUESE COMMUNICATIONS
DANGEROUS TO U.S. OR NATO

1. PROPOSAL A: That an effort be made, through the Security Coordinating Committee of the NATO Standing Group, to convince the various NATO members requiring indoctrination, including particularly the Portuguese, of the security and the adequacy of the TYPEX cryptosystem and procedures which have been authorized for the transmission of sensitive NATO information.

COMMENT

This proposal might produce either prompt or long-term remedial results but the Committee feels dubious about the efficacy of such an approach since it has no elements of shock necessary to impress the derelict NATO members. Past experience affords no basis for a belief, or even the hope that such a simple approach would be effective. The fatuous confidence which, as a general rule, those [redacted] is well known and no reliance can be placed in this approach to the problem of the insecurity of Portuguese communications containing COSMIC or NATO TOP SECRET and SECRET information.

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

2. PROPOSAL B: That a direct U.S. or U.S./U.K. approach to the Portuguese Government be made, [redacted]

[redacted] The objective would be to force immediate adherence to COSMIC security regulations, thus producing prompt remedial results, and to assure an eventual reorganization and improvement in the security of all Portuguese communications.

COMMENT

a. This proposal is practically identical with that proposed in USCIB 14/132 in regard to [redacted] and involves a direct approach to the Portuguese at the highest governmental level, viz., the Secretary of State

through the U.S. Ambassador in Lisbon to the Portuguese Minister of Foreign Affairs (MFA).

b. Such an approach necessitates bringing the COMSEC situation to the attention of the MFA in a manner so dramatic as to shock him into taking speedy and effective action.

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

c. The disadvantages of such an approach in the case of the Portuguese are:

[Redacted]

general insecurity-mindedness and loquacity of the Portuguese people as a whole make this course dangerous.

(2) In the case of [Redacted] the purpose of delivering such a shock is to bring about a drastic overhaul of the cryptosystems and practices [Redacted]

[Redacted] There is, however, not only no immediate or over-riding necessity, from the point of view of U.S. security, of bringing this about in the case of the Portuguese, [Redacted]

provided that segment of the insecurity which involves leakage of COSMIC or NATO TOP SECRET and SECRET information can be eliminated [Redacted]

3. PROPOSAL C: That a high-level approach to the Portuguese Government be made, disclosing our positive knowledge of Portuguese violations of the COSMIC security regulations [Redacted] the disclosure would be made ostensibly with a view to insisting upon Portuguese observance of those regulations, thus producing prompt remedial results.

COMMENT

This is the proposal unanimously agreed to by the Committee and is discussed in detail in paragraphs 12-15 of the basic paper.

4. PROPOSAL D: That there be established a NATO courier service which would be adequate to support the present NATO agreement that all possible COSMIC, NATO TOP SECRET and SECRET information be transmitted by pouch.

COMMENT

The Ad Hoc Committee studied the matter of greater use of courier service by NATO members and further explored the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information stating that before the information is released there must be assurances that it will not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized (see paragraph 24 of reference Report). The Committee finds that:

a. The current regulations* relative to the transmission of COSMIC information and documents (Paragraph 14, Annex "B" to D.C. 2/7) clearly require that courier service be given first priority as the means of transmission; electrical cryptographic transmission "should only be utilized when time does not permit the use of accompanied bag."

b. U.S. Air Force, Army, and State Department air courier services have been placed at the disposal of NATO governments to the limited extent that such services are available. However, even such of these services as are at their disposal are not used by the NATO governments for the transmission of national comment, since they are unwilling to rely upon the inviolability of pouches not accompanied by one of their own national couriers.

c. A NATO courier service would not only be extremely costly but also there is nothing to indicate that the NATO governments would put much confidence even in a NATO courier service unless national couriers of their own selection were provided to accompany the pouches in each case of such transmission. The availability of such couriers is questionable, in view of the expense to each government, and, moreover, there are times when electrical transmission must be used, so that the door would still be left open for security violations in such instances, since the government concerned might still use its insecure national system for national comment on COSMIC information.

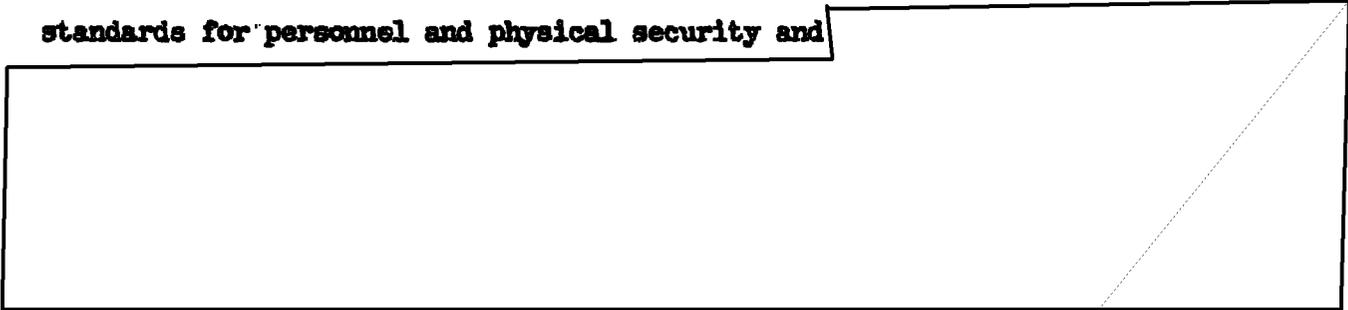
5. PROPOSAL E: That there be established a security training program, curriculum, and school for all elements of the NATO organization, both civilian and military.

* See footnote to para. 3 of this Report.

COMMENT

See comment under Proposals F and G.

6. PROPOSAL F: That a bilateral U.S.-Portuguese security survey, similar to the recently completed tripartite U.S.-U.K.-French survey, be made and that this survey include among its objectives (1) the attainment of mutually-agreed standards for personnel and physical security and



COMMENT

See comment under Proposal G.

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

7. PROPOSAL G: That an effort be made to obtain adoption throughout NATO of the Tripartite Security Standards now being considered for adoption by the U.S., U.K. and France.

COMMENT

a. The basis for Proposals E, F, and G is to be found in the following extracts from NATO documents:

(1) Para. 3 of Appendix to D.C. 2/7, 13 April 1951:*

"3. Establishment of Agencies to Control and Coordinate Security.

a. At the Standing Group Level: The Security Coordinating Committee. A Security Coordinating Committee of the Standing Group is constituted, composed of French, United States and United Kingdom representation. Security representatives of other member countries or spokesmen from Regional Security Committees will be called upon for assistance when necessary. The Security Coordinating Committee is responsible directly to the Standing Group for the supervision of security within the whole of the NATO system at all levels and for the periodic examination of the functioning thereof. Any security policy affecting NATO as a whole will require final approval at the Council level."

* See footnote to para. 3 of this Report.

(2) Para. 5 of S.G.-41/3, 10 April 1951:

"5. The Security Coordinating Committee Shall:

a. Be responsible to the Standing Group for recommendations and guidance concerning security policy.

b. Supervise and periodically examine the functioning of the NATO Security System including COSMIC registries and the COSMIC system of communication. The authority of the country to be examined will be obtained before the examination is carried out and it will be conducted by and with the assistance of the country concerned."

b. These extracts are quoted to show that periodic Security Coordinating Committee reviews of the NATO Security System and its actual manner of functioning have been specifically authorized.

c. The Ad Hoc Committee has learned that some of the NATO countries do not even have a doctrine or document dealing with such matters as physical or personnel security, let alone standards to which their authorities should strive.

d. The physical, personnel, and industrial standards of security recently elaborated by the Tripartite Group, if approved by the three Governments concerned, will be applicable only to those members of NATO; members such as Portugal will not be bound by those standards. If, however, these standards were adopted by all NATO countries, this would be conducive toward improvement in those phases of security throughout NATO. The desirability of doing so is becoming more clear as NATO is growing in strength.

e. Under the cover of such periodic reviews as those referred to in subparagraph a above, the Security Coordinating Committee, through the Standing Group, could institute enquiries with respect to the existence of national security standards and the observance of all NATO security regulations, including those dealing with the use of courier service and electrical transmission.

f. However, even if the Tripartite Security Standards were adopted throughout NATO, training in their practical application and usage will be required and courses of instruction of several weeks' duration will be necessary as an initial step. Such courses could well include not only the three above-mentioned phases of general security but also the basic elements of communication

security, and the proper usage of the authorized NATO cryptosystems. Such indoctrination should be provided at all NATO levels, including that of the Council Deputies. In order for this to be effective, continuous supervision and review of the way in which the training is being applied in practice will be necessary. It is clear, therefore, that to be fully effective, the action contemplated in these last three proposals is necessarily long-term and continuing in character.

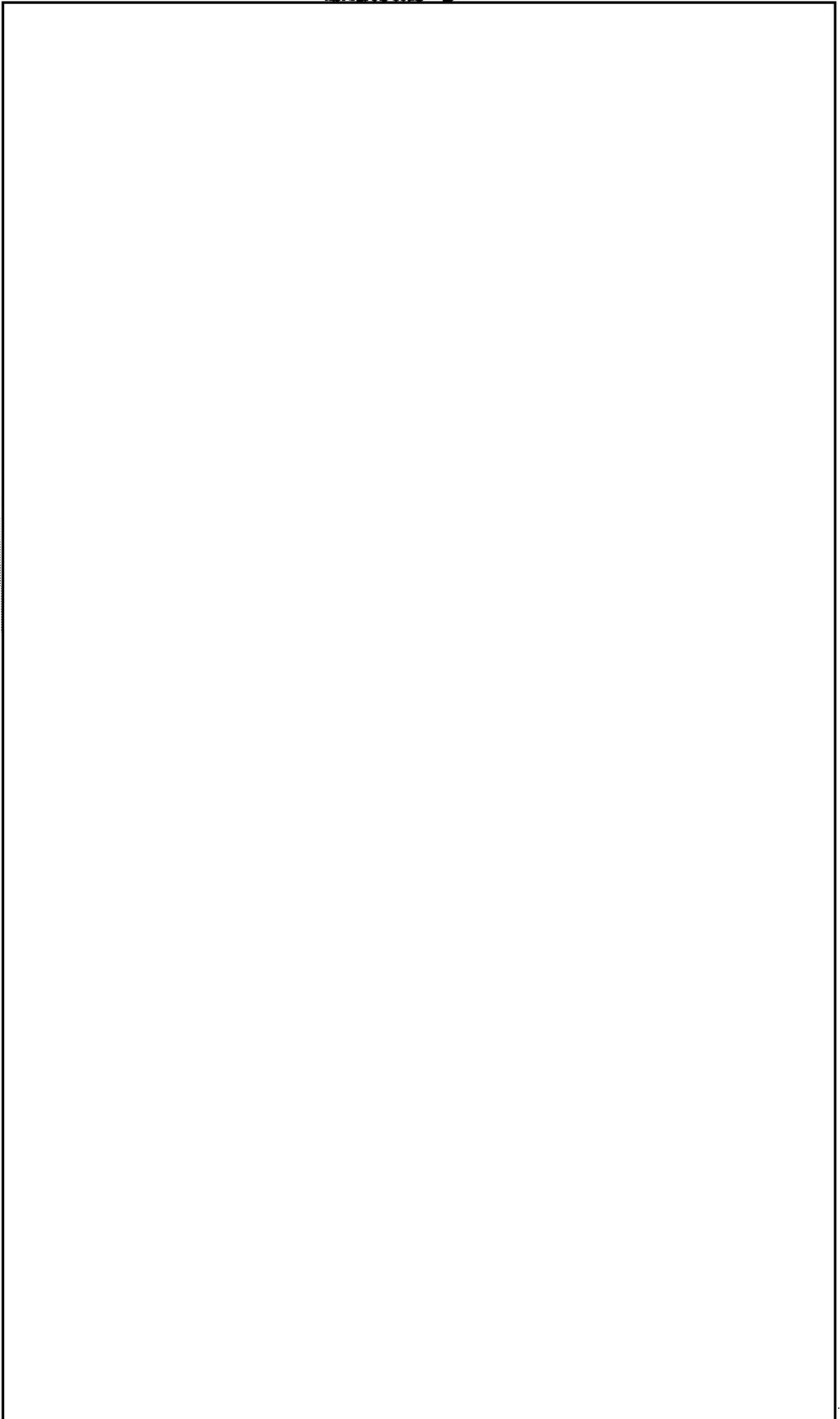
g. The Committee is of the opinion that, in regard to all the foregoing proposals, the matter must be discussed with the U.K. authorities before any approach to the Portuguese is made, especially if a proposal



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

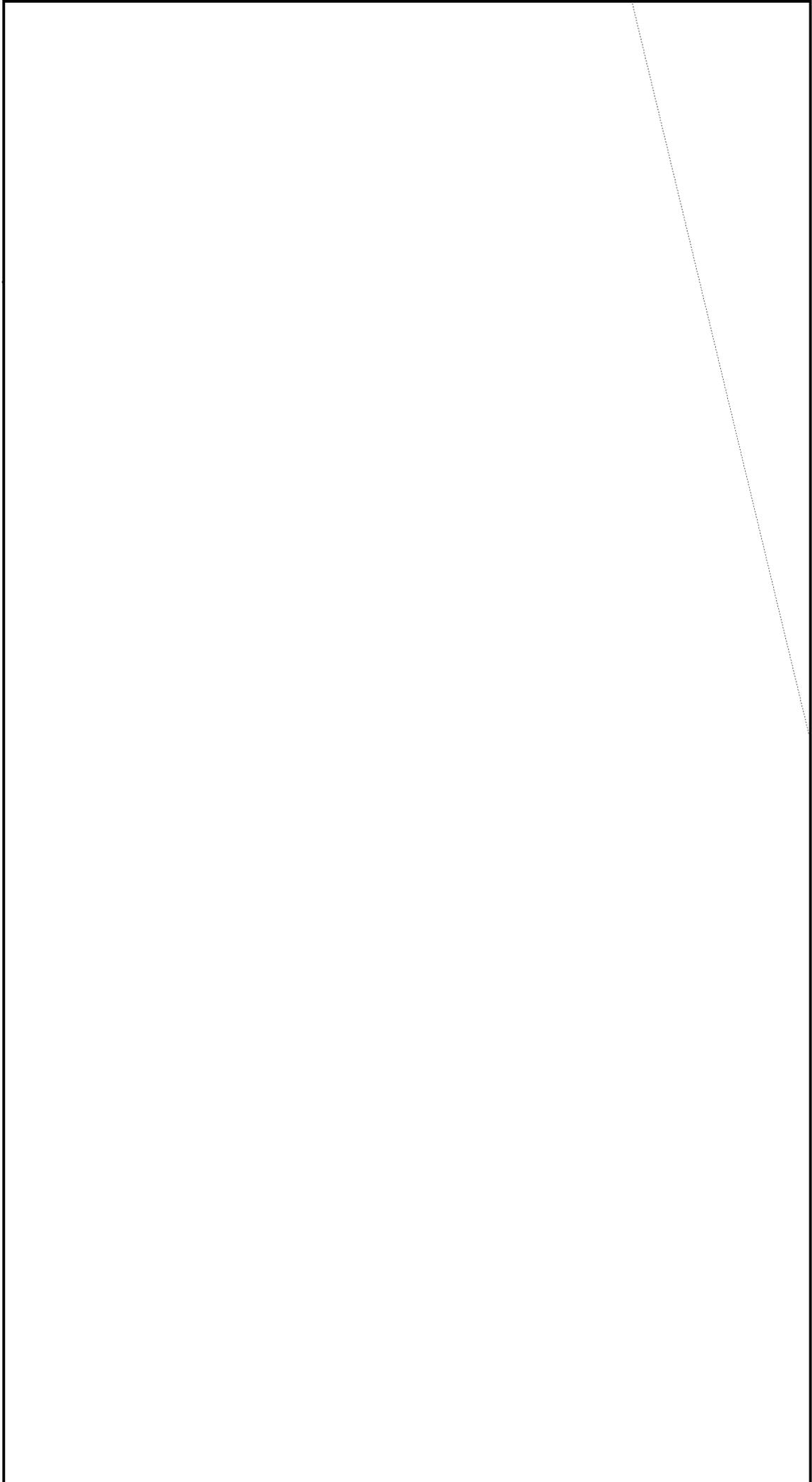
EO 3.3(h) (2)
PL 86-36/50 USC 3605

ENCLOSURE "B"



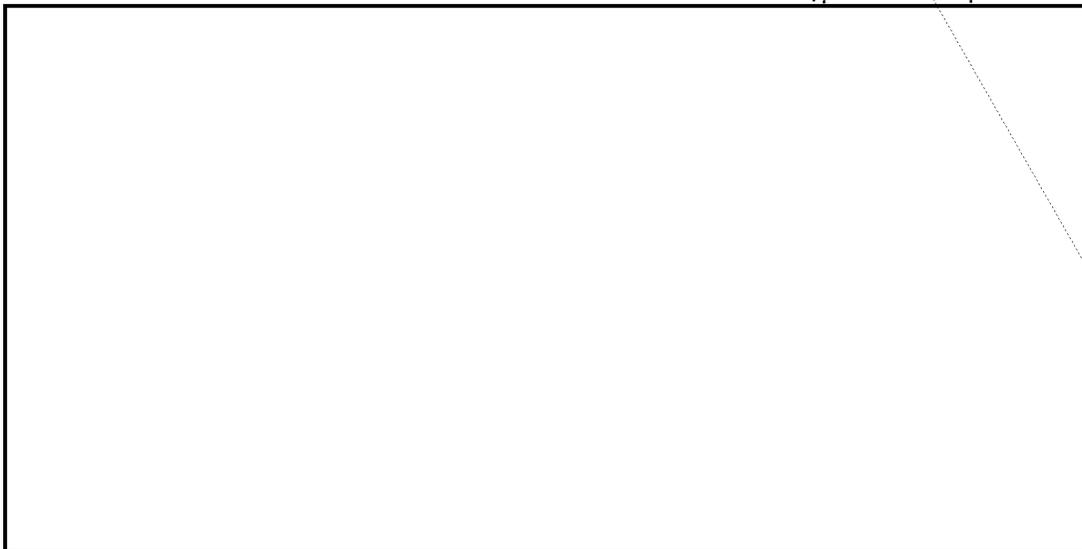
EO 3.3(h) (2)
PL 86-36/50 USC 3605

ENCLOSURE "B"



- 18 - Enclosure "B" with USCIB

ENCLOSURE "B"



* Underlining supplied.

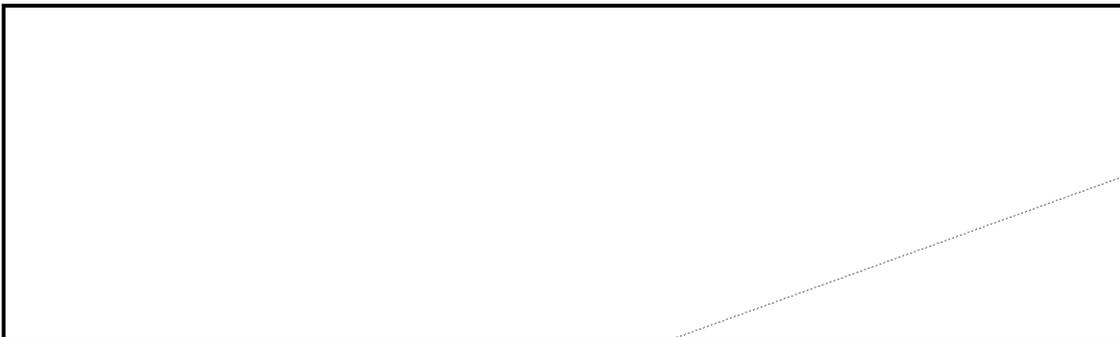
ENCLOSURE "C"

Memorandum for Chairman, London Signal Intelligence Board

Subject: Insecurity of Portuguese Communications

Enclosure: Report on Portuguese Communication Security

1. The enclosure is a Report approved by the United States Communications Intelligence Board on _____, and involves action proposed to remedy a situation dangerous to U.S. and NATO security, arising from the insecurity of certain Portuguese communications.



3. Early telegraphic reply would be appreciated.

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

ENCLOSURE "D"

Memorandum for: The Secretary of State

Subject: Proposed action by the U.S. Government in the matter of
insecurity of Portuguese communications

Enclosure: Report on Portuguese Communication Security

1. The enclosure is a Report approved by the United States Communications Intelligence Board on _____, and involves action proposed to remedy a situation dangerous to U.S. and NATO security, arising from the insecurity of certain Portuguese communications.

2. The action proposed by the United States Communications Intelligence Board as outlined in paragraph 12 of the Enclosure has received the concurrence of the London Signal Intelligence Board.

3. It is requested that the action proposed to correct the danger to U.S. and NATO arising from the insecurity of Portuguese communications, be implemented at the earliest practicable date.

27 July

at meeting on

DRAFT AS REVISED 26 JULY 1951

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

D-R-A-F-T

D-R-A-F-T

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

Reference: USCIB: 23/18

1. At its 66th Meeting, 13 July 1951, USCIB approved the referenced Report, which recommended that:

"b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government."

2. The Ad Hoc Committee has continued its study of the problem, and has developed the additional facts and conclusions set forth below.

3. The existing NATO regulations designed to protect sensitive NATO information, as set forth in D.C. 2/7, 13 April 1951, are adequate for the purpose, if strictly enforced. The definitions of "COSMIC" and "NATO" information are clear and susceptible of being applied with precision.

4. Some Portuguese communications which contain information that clearly falls within the limits stipulated by the definitions are secure, since such communications are being transmitted by the authorized crypto-systems, viz., TYPEX with simplex settings. However, even in cases where the Portuguese have used TYPEX, their lack of security and the manner in

which they use the machine make those messages possibly vulnerable to cryptanalytic attack and weaken the NATO TYPEX system as a whole.

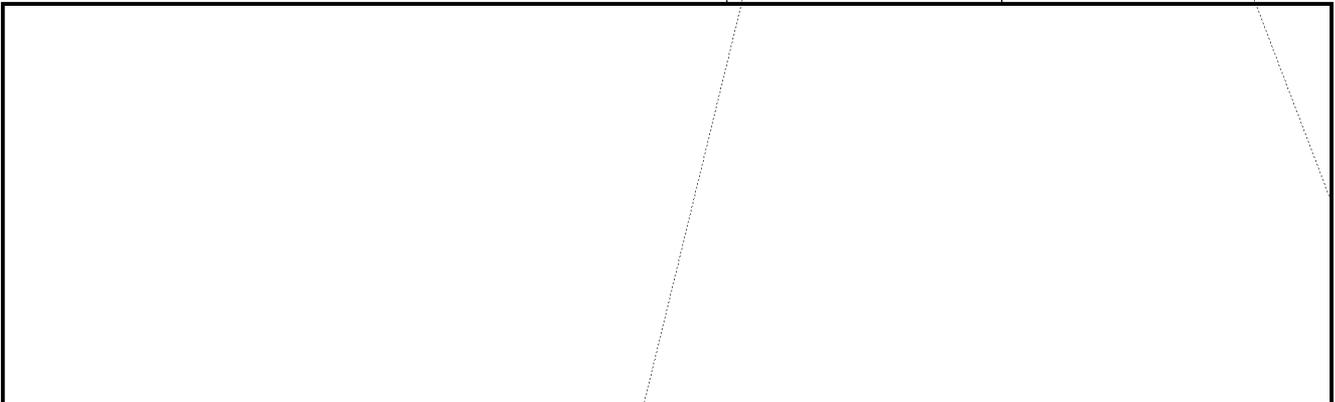
5. Some NATO communications, however, contain information which may be characterized by the designation "NATO fringe traffic", and which consists largely of national comment on COSMIC or NATO matters and documents. At the time that the definitions of COSMIC and NATO information were elaborated, the question whether national comment was to be considered COSMIC or NATO information was discussed and specific provision that it be so considered was excluded. This exclusion was at the request of the Department of State, which, inter alia, did not wish its own representatives to NATO hampered in regard to this matter. It is COSMIC material and this "fringe traffic" which constitute the principal sources of insecurity as regards NATO and U.S. information, and which, in the case of Portuguese communications, are causing serious damage to security.

6. In transmitting national comment, the Portuguese member of the Council Deputies in London (and diplomats of other NATO governments) prefer to use their own national cryptosystems rather than TYPEX because they fear that the British might read TYPEX messages, since the settings are provided by the British. In the case of Portugal, the national cryptosystem used is the Hagelin C-38 machine, with such poor procedures that the messages are easily solved. It may be assumed with some certainty that the U.S.S.R. is reading these Portuguese messages.

7. On 25 April 1951 all NATO member nations were informed by SGM-616-51 that the Signatory Nations of the North Atlantic Treaty Organization were authorized, in addition to constructing their own plugboard setting keys, to prepare individual National Books of Settings should this be desired "in order still further to preserve the discreet nature of the channels provided for National use." They were also informed at the same

time that "the U.K. have prepared a memorandum describing a secure method for the compilation of simplex settings and a copy will be made available to other member Nations if desired."

8. The Ad Hoc Committee is attempting to ascertain whether any NATO country has yet availed itself of the opportunity to compile its own "National Books of Settings", or even of the authority granted to compile its own National plugboard settings. It is obvious, however, that Portugal has not yet availed itself of either opportunity and there are no indications of an intention to do so in the near future.



10. The Ad Hoc Committee has studied the matter of greater use of courier service by NATO members. It has further explored the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information stating that before the information is released there must be assurances that it will not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized (see paragraph 24 of reference Report). In this connection the Ad Hoc Committee finds that:

a. The current regulations relative to the transmission of COSMIC information and documents (Paragraph 14, Annex "B" to D.C. 2/7) clearly require that courier service be given first priority as the means of transmission; electrical cryptographic transmission "should only be utilized when time does not permit the use of accompanied bag."



b. A NATO courier service has been considered. Such a service would cost about \$100,000 per month. Although the cost of such service might not be too great in view of the importance of keeping certain matters secure, there is nothing to indicate that the NATO governments would put much confidence even in a NATO courier service unless national couriers of their own selection were provided to accompany the pouches in each case of such transmission. The availability of such couriers is questionable, in view of the expense to each government, and, moreover, there are times when electrical transmission must be used, so that the door would still be left open for security violations in such instances, since the government concerned would still use its insecure national system for national communication on COSMIC information.

c. A better and far less expensive answer might be to provide indoctrination and training in the production of national settings and in the proper use of the TYPEX machine for COSMIC and NATO material as well as for "fringe traffic".

11. The physical, personnel, and industrial standards of security recently elaborated by the Tripartite Group, if approved by the three Governments concerned, will be applicable to only those members of NATO; members such as Portugal will not be bound by those standards. If, however, these standards were adopted by all NATO countries, this would be conducive toward improvement in those phases of security throughout NATO. The desirability of doing so is becoming more clear as NATO is growing in strength.

12. Even if those standards were adopted throughout NATO, training in their practical application and usage will be required and courses of instruction of approximately three weeks' duration will be necessary. Such courses could well include not only the three above-mentioned phases of general security but also the basic elements of communication security, and the proper usage of the authorized NATO cryptosystems.

Page Denied

17. a. Paragraph 3 of the Appendix to D.C. 2/7 reads as follows:

3. Establishment of Agencies to Control and Coordinate Security.

a. At the Standing Group level: The Security Coordinating Committee. A Security Coordinating Committee of the Standing Group is constituted, composed of French, United States and United Kingdom representation. Security representatives of other member countries or spokesmen from Regional Security Committees will be called upon for assistance when necessary. The Security Coordinating Committee is responsible directly to the Standing Group for the supervision of security within the whole of the NATO system at all levels and for the periodic examination of the functioning thereof. Any security policy affecting NATO as a whole will require final approval at the Council level."

b. Paragraph 5 of S.G.-41/3, dated 10 April 1951, reads as follows:

5. The Security Coordinating Committee shall:

a. Be responsible to the Standing Group for recommendations and guidance concerning security policy.

b. Supervise and periodically examine the functioning of the NATO Security System including COSMIC registries and the COSMIC system of communication. The authority of the country to be examined will be obtained before the examination is carried out and it will be conducted by and with the assistance of the country concerned."

c. These extracts are quoted to show that periodic Security Coordinating Committee examinations of the NATO Security System and its functioning have been specifically authorized.

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

26 July 1951

D-R-A-F-T

1st
D-R-A-F-T

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

Reference: USCIB: 23/18

1. At its 66th Meeting, 13 July 1951, USCIB approved the referenced Report, which recommended that:

"b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government."

2. The Ad Hoc Committee has continued its study of the problem, and has developed the additional facts and conclusions set forth below.

3. The existing NATO regulations designed to protect sensitive NATO information, as set forth in D.C. 2/7, 13 April 1951, are adequate for the purpose, if strictly enforced. The definitions of "COSMIC" and "NATO" information are clear and susceptible of being applied with precision.

4. Portuguese communications which contain information that clearly falls within the limits stipulated by the definitions are secure, since such communications are being transmitted by the authorized cryptosystem, viz., TYPEX with simplex settings.

5. Some NATO communications, however, contain information which may be characterized by the designation "NATO fringe traffic", and which consists largely of national comment on COSMIC or NATO matters and documents. It is this "fringe traffic" which constitutes the principal source of insecurity as regards NATO and U.S. information, and which, in the case of Portuguese communications, is causing serious damage to security. At the time that the definitions of COSMIC and NATO information were elaborated, the question whether national comment was to be considered COSMIC or NATO information was discussed and was specifically excluded from the definitions. This exclusion was at the request of the Department of State, which did not wish its own representatives to NATO hampered in regard to this matter, and at the same time did not wish to "cheat" by having its diplomatic representatives use U.S. systems contrary to the NATO agreement.

6. Such national comment is most frequently originated by officials of the Foreign Office or of the Diplomatic Corps rather than by members of the military departments of the NATO governments. This is particularly true in the case of Portugal.

7. All the TYPEX machines allocated to NATO members by the British have been distributed and are in use. However, the holders are all in the military departments of those NATO countries, and no machines have been allocated for use on the diplomatic level by members of the Foreign Offices or Diplomatic Services. However, it appears that additional allocations of TYPEX machines for use on the diplomatic level would not accomplish the objective, for the reason given in the next paragraph.

8. In transmitting national comment, the Portuguese member of the Council of Deputies in London (and diplomats of other NATO governments) prefer to use their own national cryptosystems rather than TYPEX because they fear that the British might read TYPEX messages, since the settings are provided by the British. In the case of Portugal, the national cryptosystem

used is the Hagelin C-38 machine, with such poor procedures that the messages are easily solved. It may be assumed with some certainty that the U.S.S.R. is reading these Portuguese messages.

9. On 25 April 1951 all NATO member nations were informed by SGM-616-51 that the Signatory Nations of the North Atlantic Treaty Organization were authorized, in addition to constructing their own plugboard setting keys, to prepare individual National Books of Settings should this be desired "in order still further to preserve the discreet nature of the channels provided for National use." They were also informed at the same time that "the U.K. have prepared a memorandum describing a secure method for the compilation of simplex settings and a copy will be made available to other member Nations if desired."

10. The Ad Hoc Committee has no information as to whether any NATO country has yet availed itself of the opportunity to compile its own "National Books of Settings", or even of the authority granted to compile its own National plugboard settings. It is obvious, however, that Portugal has not yet availed itself of either opportunity and there are no indications of an intention to do so in the near future.

12. The Ad Hoc Committee has studied the matter of greater use of courier service by NATO members. It has further explored "the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information stating that before the information is released there must be assurances that it will preferably not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized" (see paragraph 24 of reference Report). In this connection the Ad Hoc Committee finds that:

a. The current regulations relative to the transmission of COSMIC information and documents (Paragraph 14, Annex "B" to D.C. 2/7) clearly require that courier service be given first priority as the means of transmission; electrical cryptographic transmission "should only be utilized when time does not permit the use of accompanied bag."

b. U.S. Air Force, Army, and State Department air courier services have been placed at the disposal of NATO governments to the limited extent that such services are available. However, even such of these services as are at their disposal are not used by the NATO governments for the transmission of national comment, since they are unwilling to rely upon the inviolability of pouches not accompanied by one of their own national couriers.

c. A NATO courier service has been considered. Such a service would cost about \$100,000 per month, a fairly sizable amount with a far-flung system which is becoming larger with each additional country that enters into NATO. Although the cost of such service might not be too great in view of the importance of keeping certain matters secure, there is nothing to indicate that the NATO governments would put much confidence in even a NATO courier service unless national couriers of their own selection were provided to accompany the pouches in each case of such transmission. The availability of such couriers is questionable, in view of the expense to each government, and, moreover, there are times when electrical transmission must be used, so

that the door would still be left open for security violations in such instances, since the government concerned would still use its insecure national system for national comment on COSMIC information.

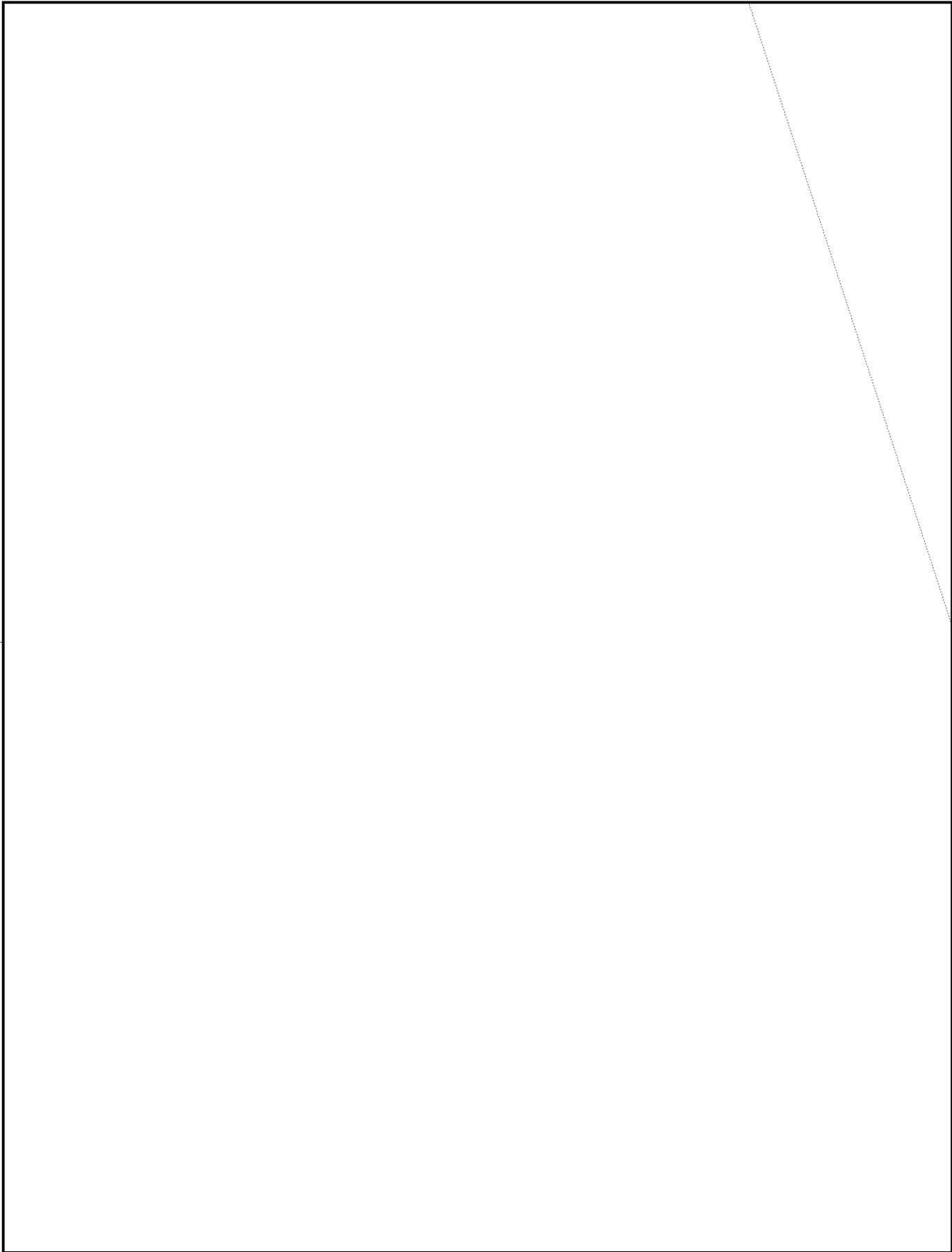
d. A better and far less expensive answer might be (1) to furnish additional TYPEX machines for use on the diplomatic level, and (2) to provide indoctrination and training in the production of national settings and in the proper use of the machines for NATO "fringe traffic" and purely national comment on communications having a bearing on NATO affairs.

13. The physical, personnel, and industrial standards of security recently elaborated by the Tripartite Group, if approved by the three governments concerned, will be applicable to only those members of NATO; members such as Portugal will not be bound by those standards. If, however, these standards were adopted by all NATO countries, this would be conducive toward improvement in those phases of security throughout NATO. The desirability of doing so is becoming more clear as NATO is growing in strength. The proposed integration into a single military force of the five separate forces of France, Italy, Western Germany, Belgium, and Luxembourg increases the importance of a single set of standards of security.

14. Even if those standards were adopted throughout NATO, training in their practical application and usage will be required and courses of instruction of approximately three weeks' duration will be necessary. Such courses could well include not only the three above-mentioned phases of general security but also the basic elements of communication security and cryptography, particularly in regard to the application and usage of the authorized NATO cryptosystems. Such courses could be established under the authority of the Council of Deputies with SHAPE designated as executive agent.

EO 3.3(h)(2)
(b)(3)-50 USC 3024(i)

15. Action such as indicated in paragraphs 13 and 14 is by its nature long-term in character, requiring at least one or two years. The current



Page Denied

with respect to the observance of the regulations in regard to the use of courier service and especially of TYPEX. In so doing the enquiries would lead naturally, and without arousing suspicion as to motives, to questions regarding the compilation of national settings for TYPEX as authorized by the Standing Group on 25 April 1951. Such queries would be all the more innocuous if it were pointed out and if it were true that the U.S. and the U.K. were using their own nationally compiled settings for TYPEX in national comment on NATO matters in view of the high security of the TYPEX system and its guarantees of privacy for purely national communications.

21. Should this plan prove feasible, the first government to be approached should be Portugal, who should be assisted in every way possible to institute the compilation and use of national settings for TYPEX at the earliest practicable moment.

22. The foregoing plan should and probably could not be instituted without prior agreement with the U.K. authorities, and negotiations with LSIB should be initiated immediately. Drafts of telegrams to the appropriate authorities are contained in the Enclosure.

ENCLOSURE "A"

Long-term Program for Introduction of Remedial Measures for a General
Improvement in the Security of NATO Communications

1. Security Coordinating Committee (SCC) of the Standing Group (SG) undertakes a review of NATO security regulations in accordance with provisions of paragraph 3 of Appendix to D.C. 2/7 and paragraph 5 of SG-41/3.
2. SCC recommends to the SG that:
 - a. The physical, personnel, and industrial security standards elaborated by the Tripartite Security Group be adopted throughout NATO and be applied throughout all NATO levels including that of the Council Deputies (CD).
 - b. With a view to insuring and facilitating strict compliance with the regulations set forth in paragraphs 14 and 17 of Annex "B" to D.C. 2/7, indoctrination of NATO authorities in the use of TYPEX be provided at all levels, including that of the CD; such indoctrination to include an explanation as to why TYPEX was selected, its proper use, compilation of National settings, etc.
3. Following approval and acceptance by the CD of step 2, the SCC recommends to the SG that there be established under the auspices of the CD, with SHAPE as executive agent, training courses of approximately three weeks' duration, such courses (1) to include not only the elements of physical, personnel and industrial security but also the basic elements of communication security and the proper use of the authorized NATO cryptosystems, and (2) to be open to military and civilian personnel selected by each NATO government on the basis of the need-to-know.

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

ENCLOSURE "B"

Program for Immediate Remedial Measures to Correct the Insecurity of
Portuguese Communications

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

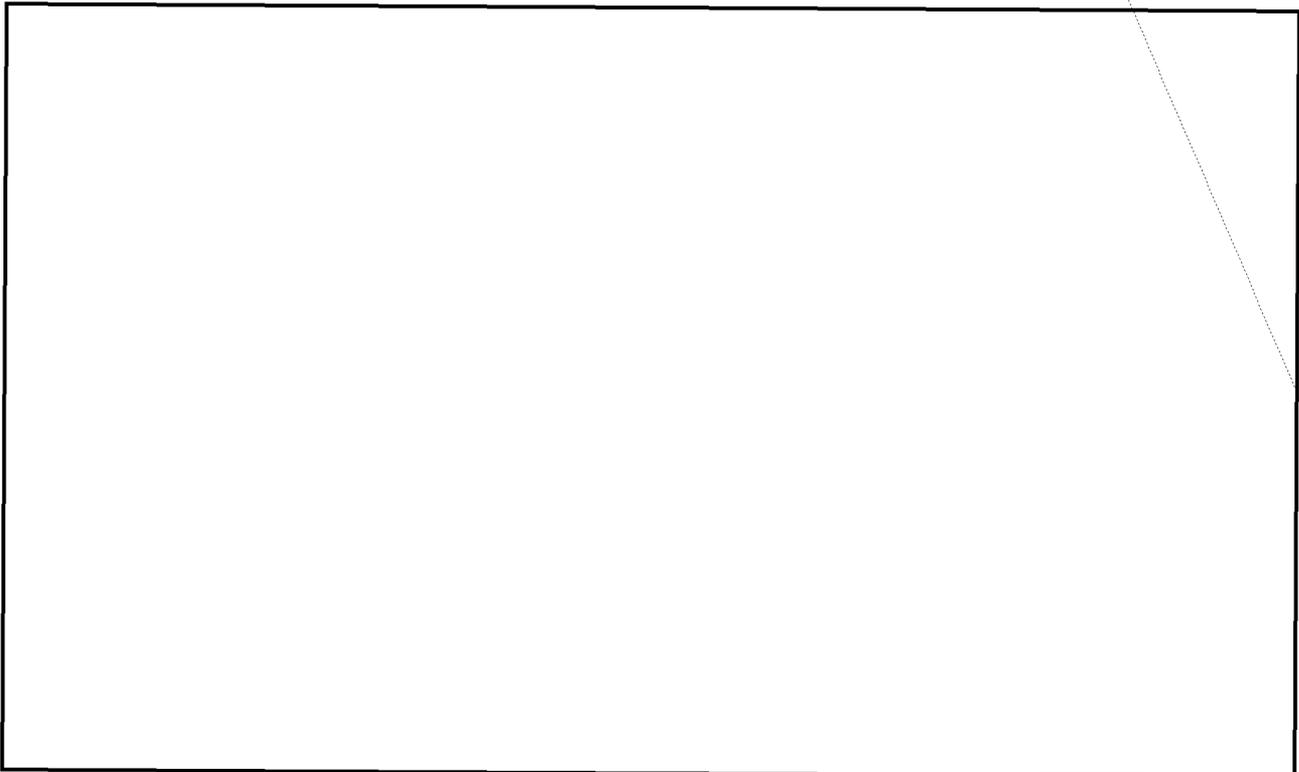
1. Following approval by the National Security Council of USCIB in regard



USCIB requests concurrence of LSIB to the making of a direct unilateral (U.S.) approach to the Portuguese Government at the highest level with a view to correcting the current insecurity of Portuguese communications dealing with NATO affairs.

2. In presenting the matter to LSIB, the proposed steps would be indicated as being the following:

a. The U.S. Secretary of State, through the U.S. Ambassador in Lisbon, notifies the Portuguese Minister of Foreign Affairs (MFA) that the U.S. Government has a report from a usually most reliable source that the



COSMIC or NATO classified information be transmitted either in TYPEX with simplex settings provided by the British or in TYPEX with simplex settings of national production.

3. Upon acceptance by LSIB of the steps outlined in paragraph 2, to make the approach to the Portuguese MFA as indicated.

~~TOP SECRET SUEDE~~
REF ID: A67137

DRAFT AS REVISED 2 AUGUST 1951

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

~~TOP SECRET SUEDE~~

REPORT OF THE USCIB AD HOC COMMITTEE

to the

UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

on

PORTUGUESE COMMUNICATION SECURITY

Reference: USCIB: 23/18

1. At its 66th Meeting, 13 July 1951, USCIB approved the referenced Report, which recommended that:

"b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government."

2. The Ad Hoc Committee has continued its study of the problem, and has developed the additional facts and conclusions set forth below.

3. The existing NATO regulations designed to protect sensitive NATO information, as set forth in D.C. 2/7, 13 April 1951, are adequate for the purpose, if strictly followed. The definitions of "COSMIC" and "NATO" information are clear and susceptible of being applied with precision.

4. Some Portuguese communications which contain information that clearly falls within the limits stipulated by the definitions are secure, since these communications are being transmitted by the authorized cryptosystems, viz., TYPEX with simplex settings. However, even in cases where the Portuguese have used TYPEX, their lack of COMSEC "know-how" and the manner in which they use the machine make those messages possibly vulnerable to cryptanalytic attack and weaken the NATO TYPEX system as a whole.

5. Some NATO communications, however, contain information which may be characterized by the designation "NATO fringe traffic", and which consists largely of national comment on "COSMIC" or "NATO" matters and documents. At the time that the definitions of COSMIC and NATO information were elaborated, the question whether national comment was to be considered COSMIC or NATO information was discussed and specific provision that it be so considered was excluded. This exclusion was at the request of the Department of State, which, inter alia, did not wish its own representatives to NATO hampered in regard to this matter. In the case of Portuguese communications, it is both COSMIC material and this "fringe traffic" which constitute the principal sources of insecurity of NATO and U.S. information.

6. In transmitting national comment, the Portuguese member of the Council Deputies in London prefers to use a Portuguese cryptosystem rather than TYPEX because he fears that the British might read TYPEX messages, since the settings are provided by the British. In the case of Portugal, the Portuguese cryptosystem used is the Hagelin C-38 machine, with such poor procedures that in all probability the U.S.S.R. and other countries are reading these Portuguese messages, even though they may be transmitted by wire systems.

7. On 25 April 1951 all NATO member nations were informed by SGM-616-51 that the Signatory Nations of the North Atlantic Treaty Organization were authorized, in addition to constructing their own plugboard setting keys, to prepare individual National Books of Settings should this be desired "in order still further to preserve the discreet nature of the channels provided for National use." They were also informed at the same time that "the U.K. have prepared a memorandum describing a secure method for the compilation of simplex settings and a copy will be made available to other member Nations if desired." The transmission of National comment by TYPEX machines with National settings is not prohibited.

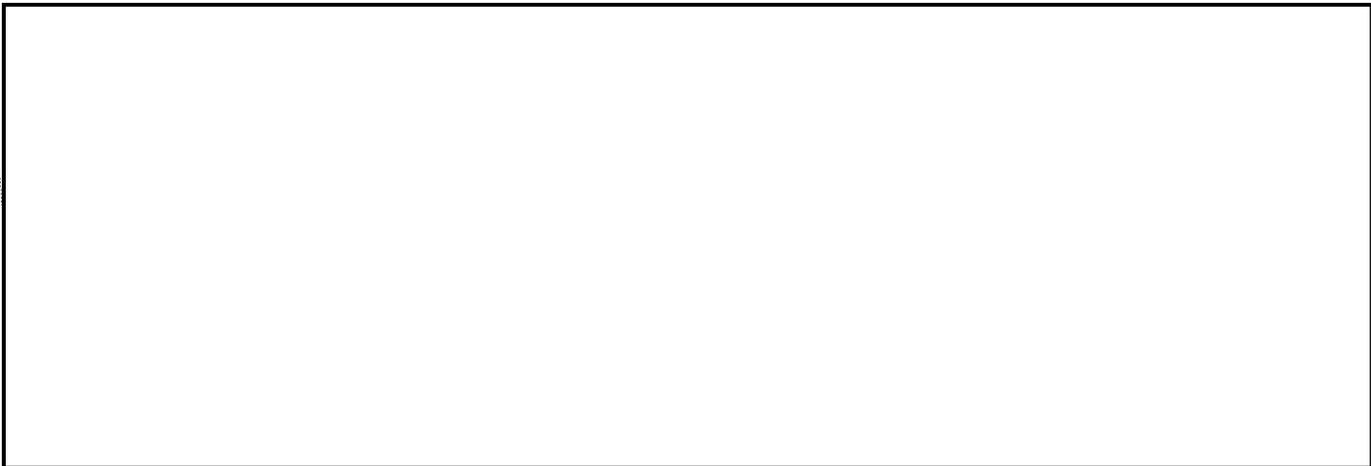
8. The Ad Hoc Committee has ascertained that not a single one of the NATO countries has yet availed itself of the opportunity to compile its own "National Books of Settings", or even of the authority granted to compile its own National plugboard settings. There are, in the case of Portugal, no indications of an intention to do so in the near future.



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

10. The Ad Hoc Committee considered a number of proposals for action which might be undertaken to correct this situation. Preliminary to its deliberations the Committee agreed that interests was almost an over-riding factor in this case, and that any solution which would definitely prejudice them should be undertaken only as a last resort. Of seven proposals worthy of serious consideration it attentively studied three which while appearing to offer the best chance of producing immediate or, at least prompt, remedial results, at the same time would present the least danger or security risk to the U.S.; the Committee then unanimously selected from among the three the one which it deems the most feasible and best under the circumstances. The proposal thus selected is described in paragraph 11 below; the remaining proposals are set forth in Enclosure "A", together with comments.

11. The selected proposal is based upon these three premises:



c. A prompt amelioration of the present insecure situation can be expected if the Portuguese could be (1) forced to comply with NATO security regulations, (2) given some indoctrination so that they would acquire full confidence in the security of TYPEX, (3) induced to make more use of the NATO authorized cryptosystem (TYPEX), and (4) take advantage of the permission granted NATO members to compile their own national books of settings for TYPEX.

12. a. The selected proposal involves a direct, and apparently unilateral (U.S.) approach on a government-to-government level, with a view to delivering a shock to the Portuguese Government by showing that:

(1) Its representative on the Council Deputies is deliberately

violating not only a well-defined NATO communication security regulation to which the Portuguese Government solemnly subscribed, but also manifests little hesitancy in disregarding an expressly stated request by the President of the Council Deputies that certain information not be transmitted by telegraph; and

(2) The security violation involved the possible disclosure of highly sensitive U.S. information of a character clearly political and of highest importance to NATO and U.S. security.



c. The Portuguese Government would be informed that the U.S. Government is so incensed and concerned about this flagrant violation directly affecting its own security, as well as that of the whole of NATO, that it is seriously considering referring the matter to the Council Deputies; however, the U.S. Government is reluctant to take such action, provided prompt steps are taken to correct the situation and assurances are given by the Portuguese Government that the action it will take will prevent a repetition of such violation and disregard of security procedures.

d. These assurances must comprise:

(1) Assurance that the authorized NATO cryptosystem (TYPEX) will hereafter be used for the transmission of all COSMIC, TOP SECRET and SECRET NATO information, and national comment on such information; and

(2) Assurance that a request, by a government tabling information before a NATO body, that such information be transmitted only by courier will be strictly observed.

e. The Portuguese authorities would then be given positive assurance

that the TYFEX is a secure means of communication [redacted]

[redacted] This could be done merely by pointing out that TYFEX was selected by the NATO Council after due deliberation because of the high degree of security it affords when properly used. They should then be induced (1) to direct the cryptographic bureau of the Ministry of Foreign Affairs (MFA) to compile national settings for Portuguese TYFEX communications and (2) to issue a directive that when transmission by accompanied bag is not feasible because of the time factor and electrical transmission must be employed, all Portuguese communications dealing directly or indirectly with COSMIC or TOP SECRET AND SECRET NATO information will be transmitted either in TYFEX with simplex settings provided by the British or in TYFEX with simplex settings of national production.

13. The Ad Hoc Committee is unanimous in its opinion that this proposal should be adopted, for the following reasons:

a. It appears to offer the only program for prompt remedial action which affords both security and a reasonable prospect of being effective. It is recognized that to be effective, any approach to the Portuguese on this subject must shock them. This "shock" must be of such a nature that it will insure their compliance with NATO security regulations governing the transmission of classified NATO information, [redacted]

[redacted] will produce this "shock", for these messages contain these important elements: (1) a violation of a specific request by the President of the Council Deputies not to transmit the information by electrical means; (2) a statement clearly indicating that the Portuguese representative arrogates to himself the capability of reversing a judgment of the President of the Council Deputies as to the necessity for secrecy; and (3) a statement revealing the Portuguese attitude on the use of TYFEX.

b. The threatened action, viz., to bring the violation to the attention of the Council Deputies, would no doubt greatly alarm the

Portuguese Government and it would probably consent to almost any reasonable request if doing so would avoid such action.

d. It also provides an excellent opportunity to indoctrinate the Portuguese at the highest level in the actual security of the TYPEx system; it will be conducive to getting the Portuguese to use it for COSMIC, TOP SECRET and SECRET NATO information; and it will probably lead them to compiling their own TYPEx settings for transmitting national comment on such information.

14. It will be necessary to obtain the concurrence of LSIB to this proposal, which should be communicated to that Board without delay if it is accepted by USCIB. A draft of a suitable telegram is contained in Enclosure "C".

15. a. The Ad Hoc Committee is of the opinion that the approach to the Portuguese outlined in Paragraph 12 can be undertaken without referring the matter to the National Security Council (NSC) and without awaiting the

NSC decision on USCIB: 14/132

b. The Committee also feels that the exact details of making the approach, the specific U.S. official or officials to be designated to make the approach, and the specific Portuguese official or officials to be approached, should be decided by the Department of State. A draft of a suitable memorandum to the Secretary of State is set forth in Enclosure "D".

16. The Ad Hoc Committee considers that:

a. All the other proposals set forth in Enclosure "A", except Proposal B [redacted], are suitable only as long-term programs;

b. It would be advisable to initiate action on one or more of those proposals as promptly as practicable so as to assure and extend the benefits which may flow from the execution of the Ad Hoc Committee's selected proposal for immediate action, as outlined in paragraph 12; and

c. Such long-term action may also lay the ground-work for Proposal B should it become necessary to resort to that proposal.

17. The Ad Hoc Committee further considers that, except for Proposal B, all the proposals outlined in Enclosure "A", while of interest to USCIB, do not fall strictly within the cognizance of USCIB, and should be studied in detail by the proper body or bodies of NATO. It may be noted that several of the long-term proposals are interdependent in the sense that they would reinforce one another and would be most effective if undertaken together under the same authorities. With this in view the memorandum set forth in Enclosure "E" has been prepared.

18. Finally, with reference to the directive given the Ad Hoc Committee in USCIB: 23/18 to explore the possibility of instituting safeguards involving greater use of courier service and of bringing this about through an approach to the Commander of SHAPE, the Ad Hoc Committee wishes to point out that the present Portuguese insecurity involves communications which are on the diplomatic level and not between military personnel. For this reason the matter is one in which SHAPE has no jurisdiction, and an approach through SHAPE would not only be inadvisable but also very probably quite ineffective in bringing about the results desired.

RECOMMENDATIONS

19. It is recommended that:

a. The action proposed in Paragraphs 12, 14, 15, and 17, and Enclosures "C", "D", and "E" be approved;

b. The Ad Hoc Committee be directed to maintain contact with this problem in order to inform USCIB from time to time as to progress made in its solution and to notify USCIB when a satisfactory level of communication security has been attained by the Portuguese in the transmission of classified information affecting the security of the U.S. and NATO.

PROPOSALS STUDIED BY THE AD HOC COMMITTEE
TO CORRECT THE
INSECURITY OF PORTUGUESE COMMUNICATIONS
DANGEROUS TO U.S. OR NATO

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

1. PROPOSAL A: That a non-intensive effort be made, through the Security Coordinating Committee of the NATO Standing Group, to convince the various NATO members requiring indoctrination, including particularly the Portuguese, of the security and the adequacy of the TYPEX cryptosystem and procedures which have been authorized for the transmission of sensitive NATO information.

COMMENT

This proposal might produce either prompt or long-term remedial results but the Committee feels dubious about the efficacy of such an approach since it has no elements of shock necessary to impress the derelict NATO members. Past experience affords no basis for a belief, or even the hope that such a simple approach would be effective. The fatuous confidence which, as a general rule, [redacted]

[redacted] is well known and no reliance can be placed in this approach to the problem of the insecurity of Portuguese communications containing COSMIC or TOP SECRET and SECRET NATO information.

2. PROPOSAL B: That a direct U.S. or U.S./U.K. approach to the Portuguese Government be made, [redacted]

[redacted] The objective would be to force immediate adherence to COSMIC security regulations, thus producing prompt remedial results, and to assure an eventual reorganization and improvement in the security of all Portuguese communications.

COMMENT

a. This proposal is practically identical with that proposed in USCIB: 14/132 in regard [redacted] and involves a direct approach to the Portuguese at the highest governmental level, viz., the Secretary of State

through the U.S. Ambassador in Lisbon to the Portuguese Minister of Foreign Affairs (MFA).

b. Such an approach necessitates bringing the COMSEC situation to the attention of the Minister of Foreign Affairs in a manner so dramatic as to shock him into taking speedy and effective action.

c. The disadvantages of such an approach in the case of the Portuguese are:

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

[Redacted]

The general insecurity-mindedness and loquacity of the Portuguese people as a whole makes this course dangerous.

(2) In the case of [Redacted] the purpose of delivering such a shock is to bring about a drastic overhaul of the cryptosystems and practices of [Redacted]

[Redacted] There is, however, not only no immediate or over-riding necessity, from the point of view of U.S. security, of bringing this about in the case of the Portuguese, but also it would

[Redacted]

[Redacted] provided that segment of the insecurity which involves leakage of COSMIC or NATO SECRET and TOP SECRET information can be eliminated without a complete overhaul of Portuguese cryptosystems and practices.

3. PROPOSAL C: That a high-level approach to the Portuguese Government be made, disclosing our positive knowledge of Portuguese violations of the COSMIC security regulations [Redacted] sources; the disclosure would be made ostensibly with a view to insisting upon Portuguese observance of those regulations, thus producing prompt remedial results.

COMMENT

This is the proposal unanimously agreed to by the Committee and is discussed in detail in paragraphs 12-15 of the basic paper.

4. PROPOSAL D: That there be established a NATO courier service which would be adequate to support the present NATO agreement that all possible COSMIC, TOP SECRET and SECRET NATO information be transmitted by pouch.

COMMENT

The Ad Hoc Committee studied the matter of greater use of courier service by NATO members and further explored the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information stating that before the information is released there must be assurances that it will not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized (see paragraph 24 of reference Report). The Committee finds that:

a. The current regulations relative to the transmission of COSMIC information and documents (Paragraph 14, Annex "B" to D.C. 2/7) clearly require that courier service be given first priority as the means of transmission; electrical cryptographic transmission "should only be utilized when time does not permit the use of accompanied bag."

b. U.S. Air Force, Army, and State Department air courier services have been placed at the disposal of NATO governments to the limited extent that such services are available. However, even such of these services as are at their disposal are not used by the NATO governments for the transmission of national comment, since they are unwilling to rely upon the inviolability of pouches not accompanied by one of their own national couriers.

c. A NATO courier service would not only be extremely costly but also there is nothing to indicate that the NATO governments would put much confidence even in a NATO courier service unless national couriers of their own selection were provided to accompany the pouches in each case of such transmission. The availability of such couriers is questionable, in view of the expense to each government, and, moreover, there are times when electrical transmission must be used, so that the door would still be left open for security violations in such instances, since the government concerned might still use its insecure National system for National comment on COSMIC information.

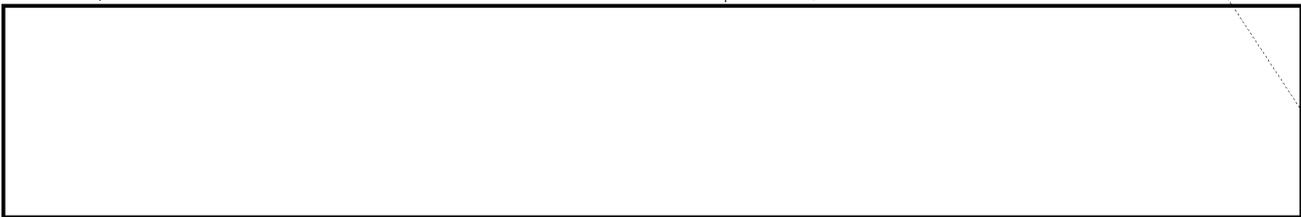
5. PROPOSAL E: That there be established a security training program, curriculum, and school for all elements of the NATO organization, both civilian and military. [LONG-TERM RESULTS.]

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

COMMENT

See comment under Proposals F and G.

6. PROPOSAL F: That a bilateral U.S.-Portuguese security survey, similar to the recently completed tripartite U.S.-U.K.-French survey, be made and that this survey include among its objectives (1) the attainment of mutually-agreed standards for personnel and physical security and (2) the



COMMENT

See comment under Proposal G.

7. PROPOSAL G: That an effort be made to obtain adoption throughout NATO of the Tripartite security standards now being considered for adoption by the U.S., U.K. and France. [LONG-TERM RESULTS.]

COMMENT

a. The basis for Proposals E, F, and G is to be found in the following extracts from NATO documents:

(1) Par. 3 of Appendix to D.C. 2/7, 13 April 1951:

"3. Establishment of Agencies to Control and Coordinate Security.

a. At the Standing Group Level: The Security Coordinating Committee. A Security Coordinating Committee of the Standing Group is constituted, composed of French, United States and United Kingdom representation. Security representatives of other member countries or spokesmen from Regional Security Committees will be called upon for assistance when necessary. The Security Coordinating Committee is responsible directly to the Standing Group for the supervision of security within the whole of the NATO system at all levels and for the periodic

examination of the functioning thereof. Any security policy affecting NATO as a whole will require final approval at the Council level."

(2) Par. 5 of S.G.-41/3, 10 April 1951:

"5. The Security Coordinating Committee shall:

a. Be responsible to the Standing Group for recommendations and guidance concerning security policy.

b. Supervise and periodically examine the functioning of the NATO Security System including COSMIC registries and the COSMIC system of communication. The authority of the country to be examined will be obtained before the examination is carried out and it will be conducted by and with the assistance of the country concerned."

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

b. These extracts are quoted to show that periodic Security Coordinating Committee reviews of the NATO Security System and its actual manner of functioning have been specifically authorized.

c. The Ad Hoc Committee has learned that some of the NATO countries do not even have a doctrine or document dealing with such matters as physical or personnel security, let alone standards to which their authorities should strive.

d. The Committee is of the opinion that, in regard to the subject of physical and personnel security, a unilateral (U.S.) approach to the Portuguese Government would offer advantages.



This applies to

Proposals B, C, and F.

e. The physical, personnel, and industrial standards of security recently elaborated by the Tripartite Group, if approved by the three Governments concerned, will be applicable only to those members of NATO;

members such as Portugal will not be bound by those standards. If, however, these standards were adopted by all NATO countries, this would be conducive toward improvement in those phases of security throughout NATO. The desirability of doing so is becoming more clear as NATO is growing in strength.

f. Under the cover of such periodic reviews as those referred to in subparagraphs a and b, the Security Coordinating Committee could work through the Standing Group to institute enquiries with respect to the existence of national security standards and the observance of all NATO security regulations, including those dealing with the use of courier service and electrical transmission.

g. However, even if the Tripartite security standards were adopted throughout NATO, training in their practical application and usage will be required and courses of instruction of several weeks' duration will be necessary as an initial step. Such courses could well include not only the three above-mentioned phases of general security but also the basic elements of communication security, and the proper usage of the authorized NATO cryptosystems. Such indoctrination should be provided at all NATO levels, including that of the Council Deputies. In order for this to be effective continuous supervision and review of the ways in which the training is being applied in practice will be necessary. It is clear, therefore, that to be fully effective, the action contemplated in these last three proposals is necessarily long-term and continuing in character.

h. It is also obvious that several of the long-term proposals are interdependent in the sense that they would reinforce one another and would be most effective if undertaken together.

i. Following approval of the Council Deputies, there could be set up under SHAPE, in order to afford instruction in the standards of security elaborated by the Tripartite Group, a training course of approximately three weeks for individuals selected by the different NATO countries; such a course to include not only elements of physical, personnel and industrial security but also the basic elements of communication security and cryptography, particularly in regard to the application and usage of authorized NATO cryptographic systems.

j. Action such as that contemplated in Proposals A, D, E, F, and G does not fall strictly within the cognizance of USCIB but of NATO authorities. Hence, such proposals should be referred to those authorities as being of interest to USCIB but for the consideration and action by NATO.

DRAFT AS REVISED 27 JULY 1951

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

REPORT OF THE USCIB AD HOC COMMITTEE
to the
UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD
on
PORTUGUESE COMMUNICATION SECURITY

Reference: USCIB: 23/18

1. At its 65th Meeting, 13 July 1951, USCIB approved the referenced Report, which recommended that:

"b. The U.S. Delegation to the U.S.-U.K. Conference on French communications security be continued as an ad hoc body to ascertain the exact extent to which present NATO practices may provide secure ways and means, within the framework of these practices, to solve the Portuguese problem.

c. Further consideration of exceptional, direct action to improve Portuguese communications security be deferred pending (1) completion of the study recommended under b above and (2) NSC and USCIB decisions whether such action is to be taken vis-a-vis the French Government."

2. The Ad Hoc Committee has continued its study of the problem, and has developed the additional facts and conclusions set forth below.

3. The existing NATO regulations designed to protect sensitive NATO information, as set forth in D.C. 2/7, 13 April 1951, are adequate for the purpose, if strictly enforced. The definitions of "COSMIC" and "NATO" information are clear and susceptible of being applied with precision.

4. Some Portuguese communications which contain information that clearly falls within the limits stipulated by the definitions are secure, since these communications are being transmitted by the authorized crypto-systems, viz., TYPEX with simplex settings. However, even in cases where the Portuguese have used TYPEX, their lack of security and the manner in

which they use the machine make those messages possibly vulnerable to cryptanalytic attack and weaken the NATO TYPEX system as a whole.

5. Some NATO communications, however, contain information which may be characterized by the designation "NATO fringe traffic", and which consists largely of national comment on COSMIC or NATO matters and documents. At the time that the definitions of COSMIC and NATO information were elaborated, the question whether national comment was to be considered COSMIC or NATO information was discussed and specific provision that it be so considered was excluded. This exclusion was at the request of the Department of State, which, inter alia, did not wish its own representatives to NATO hampered in regard to this matter. In the case of Portuguese communications, it is COSMIC material and this "fringe traffic" which constitute the principal sources of insecurity as regards NATO and U.S. information.

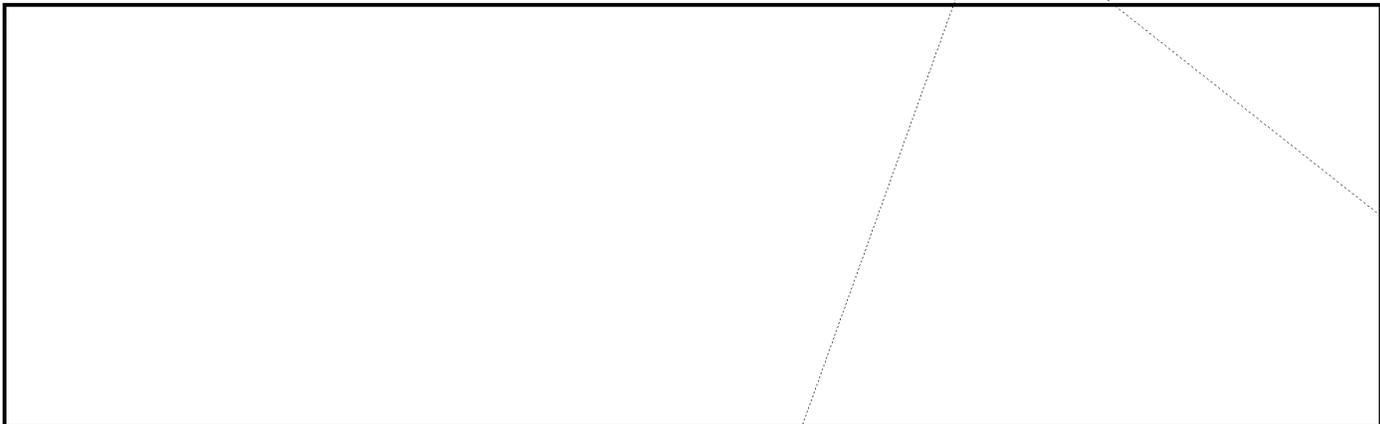
6. In transmitting national comment, the Portuguese member of the Council Deputies in London (and diplomats of other NATO governments) prefer to use their own national cryptosystems rather than TYPEX because they fear that the British might read TYPEX messages, since the settings are provided by the British. In the case of Portugal, the national cryptosystem used is the Hagelin C-38 machine, with such poor procedures that the U.S.S.R. is reading these Portuguese messages, even though they may be transmitted by wire systems.

7. On 25 April 1951 all NATO member nations were informed by SGM-616-51 that the Signatory Nations of the North Atlantic Treaty Organization were authorized, in addition to constructing their own plugboard setting keys, to prepare individual National Books of Settings should this be desired "in order still further to preserve the discreet nature of the channels provided for National use." They were also informed at the same

time that "the U.K. have prepared a memorandum describing a secure method for the compilation of simplex settings and a copy will be made available to other member Nations if desired." The transmission of National comment by TYPEX machines with National settings is not prohibited.

8. The Ad Hoc Committee is attempting to ascertain whether any NATO country has yet availed itself of the opportunity to compile its own "National Books of Settings", or even of the authority granted to compile its own National plugboard settings. It is obvious, however, that Portugal has not yet availed itself of either opportunity and there are no indications of an intention to do so in the near future.

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



10. The Ad Hoc Committee has studied the matter of greater use of courier service by NATO members. It has further explored the possibility of instituting safeguards in the form of a note to recipients of sensitive NATO information stating that before the information is released there must be assurances that it will not be forwarded by any electrical communication means; but if necessary to forward, that secure courier service would be utilized (see paragraph 24 of reference Report). In this connection the Ad Hoc Committee finds that:

a. The current regulations relative to the transmission of COSMIC information and documents (Paragraph 14, Annex "B" to D.C. 2/7) clearly require that courier service be given first priority as the means of transmission; electrical cryptographic transmission "should only be utilized when time does not permit the use of accompanied bag."



b. A NATO courier service has been considered. Such a service would cost about \$100,000 per month. Although the cost might not be too great in view of the importance of keeping certain matters secure, there is nothing to indicate that the NATO governments would put much confidence even in a NATO courier service unless national couriers of their own selection were provided to accompany the pouches in each case of such transmission. The availability of such couriers is questionable, in view of the expense to each government, and, moreover, there are times when electrical transmission must be used, so that the door would still be left open for security violations in such instances, since the government concerned might still use its insecure National system for National comment on COSMIC information.

c. A better and far less expensive answer would be to instill confidence of NATO members in the security of the TYPEX system, and to provide indoctrination and training in the production of National settings and in the proper use of the TYPEX machine for COSMIC and NATO material as well as for "fringe traffic".

11. The physical, personnel, and industrial standards of security recently elaborated by the Tripartite Group, if approved by the three Governments concerned, will be applicable to only those members of NATO; members such as Portugal will not be bound by those standards. If, however, these standards were adopted by all NATO countries, this would be conducive toward improvement in those phases of security throughout NATO. The desirability of doing so is becoming more clear as NATO is growing in strength.

12. Even if those standards were adopted throughout NATO, training in their practical application and usage will be required and courses of instruction of approximately three weeks' duration will be necessary. Such courses could well include not only the three above-mentioned phases of general security but also the basic elements of communication security, and the proper usage of the authorized NATO cryptosystems. Such indoctrination should be provided at all NATO levels, including that of the Council Deputies.

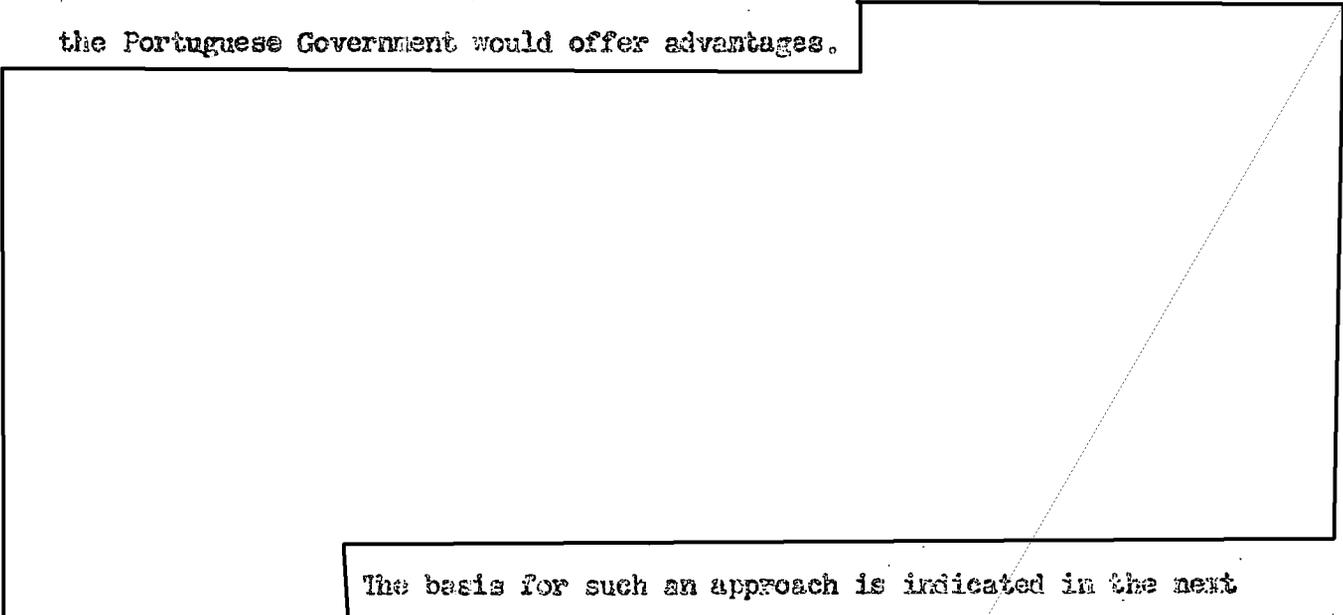
13. To be fully effective, the action indicated in paragraphs 11 and 12 must be long-term in character. The current damage to U.S. and NATO security, arising from the violation of COSMIC regulations and the insecurity of Portuguese communications, is, however, so great that prompt action is necessary.

14. The Portuguese problem resolves itself into two main phases:

a. Leading the Portuguese to introduce improvements in their security arrangements; and

b. Inducing the Portuguese to compile their own National TYPEX settings and to use TYPEX for messages containing COSMIC, NATO TOP SECRET and SECRET information or National comment on NATO matters; for until and unless they do so the current damage to NATO and U.S. security will not only continue but will increase.

15. The Ad Hoc Committee is of the opinion that, in regard to the subject of physical and personnel security, a unilateral (U.S.) approach to the Portuguese Government would offer advantages.



The basis for such an approach is indicated in the next paragraph.

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