

~~TOP SECRET~~

24

USCIB: 23/55

APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL

20 May 1953

TOP SECRET - SECURITY INFORMATIONMEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Allied (NATO) Communications Security.

1. The enclosure contains the final report of the ad hoc committee established by USCIB to examine the subject problem. This report is scheduled for consideration at a special meeting of the Board.

2. Attention is invited to the fact that the "U.S. Personnel Only" classification is required by a limited number of specific comments, which can be excised or amended without undue difficulty in the event of a decision to forward the report to



3. Pursuant to agreement by members of the ad hoc committee the distribution of this report is limited to the number of copies indicated below. This distribution is based upon the requirement expressed to the Secretariat by individual USCIB members. For purposes of record a normal distribution of this covering memorandum is being made:

Number of Copies of the Report Distributed

State	1
Defense	EO 3.3(h)(2)
FBI	PL 86-36/50 USC 3605
NSA	3
Army	4
Navy	3
Air Force	1
CIA	4

EO 3.3(h)(2)



Acting Executive Secretary, USCIB

Enclosure
Copy Number 20
of subject report.

APPENDED DOCUMENTS CONTAIN
CODE WORD MATERIAL

USCIB: 23/55

~~TOP SECRET~~

~~TOP SECRET SECURITY INFORMATION~~ **CANOE**
DEPARTMENT OF STATE

Washington 25, D.C.

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

U. S. PERSONNEL ONLY

18 May 1953

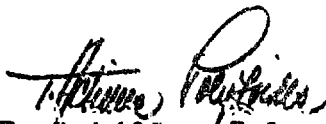
MEMORANDUM FOR THE CHAIRMAN, USCIB

SUBJECT: Report of Ad Hoc Committee on Allied
[NATO] Communications Security.

1. Transmitted herewith is the final Report of the Ad Hoc Committee established at the 82nd meeting of USCIB to examine the problem of Allied [NATO] communications security.

2. The Report includes a review of previous USCIB actions with reference to [redacted] communications security matters. This review was prepared by the Chairman of the Security Committee, USCIB at the request of the Chairman of the Ad Hoc Committee and is presented as a convenience to the Board members in their consideration of the entire subject.

3. This Report has been approved unanimously by the members of the Ad Hoc Committee.


T. Achilles Polyzoides
Chairman, Ad Hoc Committee

One enclosure, with
Tabs A through E, and
Exhibits 1, 2 and 3.

~~TOP SECRET CANOE~~

~~TOP SECRET SECURITY INFORMATION~~ **CANOE**

Copy No. 20

*Comments by
F. Austin Jones
Polyzoides Committee
Report*

~~TOP SECRET CANOE~~

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

1. There are two questions which require to be answered, the second depending on the answer to the first.

a. Can we cut off supply of consumers?

b. If so, what steps do we take to improve communication security in the national communications of NATO countries?

2. This report in its conclusions appears to give a negative answer to the first question.

3. Indeed, throughout the report there is evidence that although the "leaked"

to the U.S.

5. In other words compliance with the recommendations will result in

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

to the fact that many [redacted] only because of bad procedures. We remove the bad procedures and those [redacted] As we increase cryptographic knowledge, as we certainly will as we improve procedure, other systems basically insecure will be reexamined and removed from use. We will probably be asked to evaluate some of them and then will have to recommend against their use.

6. This report therefore seems to argue against itself and we still haven't the answer to the first question. [redacted] If the answer is no the recommendations are valueless, and it would also be futile to go on with the BRUSA conference.

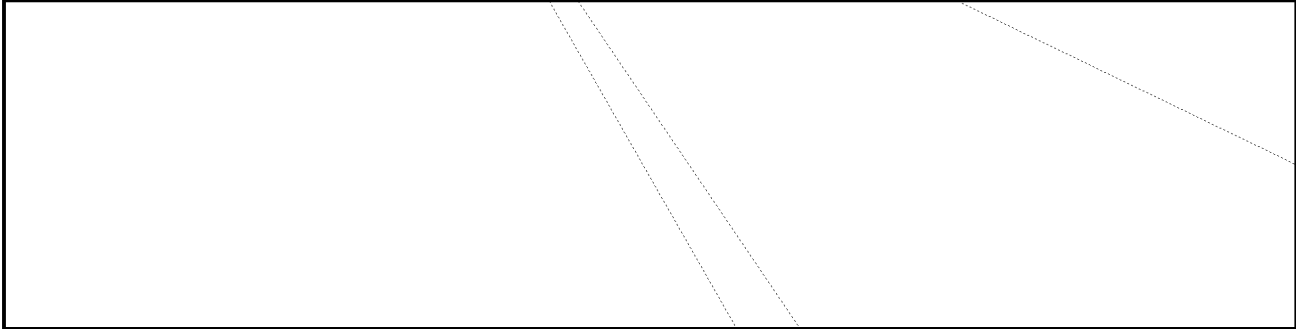
7. If the answer is yes then the recommendations are valid. The report should be changed to make this perfectly clear, and the conference must by all means proceed in order to map out the details of implementation of the recommendations.

9. One more point in the report. It fails to mention that on the military side NATO countries have been provided NATO cryptosystems in some quantity, and that that is the reason why the military picture is relatively

~~TOP SECRET CANOE~~

Wright

There is, however, always the one NATO COMSEC security regulation that is apt to be broken and that is the use of NATO systems instead of ^{mandatory}



10. It seems that there are two possible courses.

a. Modify the report to recommend against [redacted] to the U.S. and call off the UK conference, or

b. Modify the report to admit the loss of [redacted] let the recommendations stand, and let the conference proceed.

I recommend the latter course.

~~TOP SECRET~~ SECURITY INFORMATION

D R A F T

U. S. POSITION PAPER ON

CONFERENCE ON THE SECURITY OF [redacted]

1. Three issues are involved in the forthcoming U. S. - U. K. Conference on [redacted]

a. Review of proposed tactics governing an approach to the

[redacted]

[redacted]

2. Only item 1a will be considered in this paper. The general U. S. position on this item was established when the President approved the report of the U. S. - U. K. Conference on the Security of [redacted] By this approval, the U. S. was committed, subject to an improvement in the general security of the [redacted] to an approach to the [redacted] Ministry of Foreign Affairs (MFA) on the insecurity of [redacted] communications. USCIB observed to [redacted] that an approach to the [redacted] should not be made until the Tripartite Security Report was approved by each of the participating countries, and the [redacted] had undertaken definite implementing action to carry out the recommendations of the report.

3. The three governments have subsequently formally subscribed to the principles and standards of security proposed by the Tripartite Working Group, and the recommendations with respect thereto are being progressively implemented. The U. S. and U. K. delegations to a recent conference of the Tripartite Working Group have agreed, in spite of reservations about Civil Ministries, that positive steps are being taken by the [redacted] to put into effect these principles and standards. The U. S. must decide whether the "positive steps" already taken

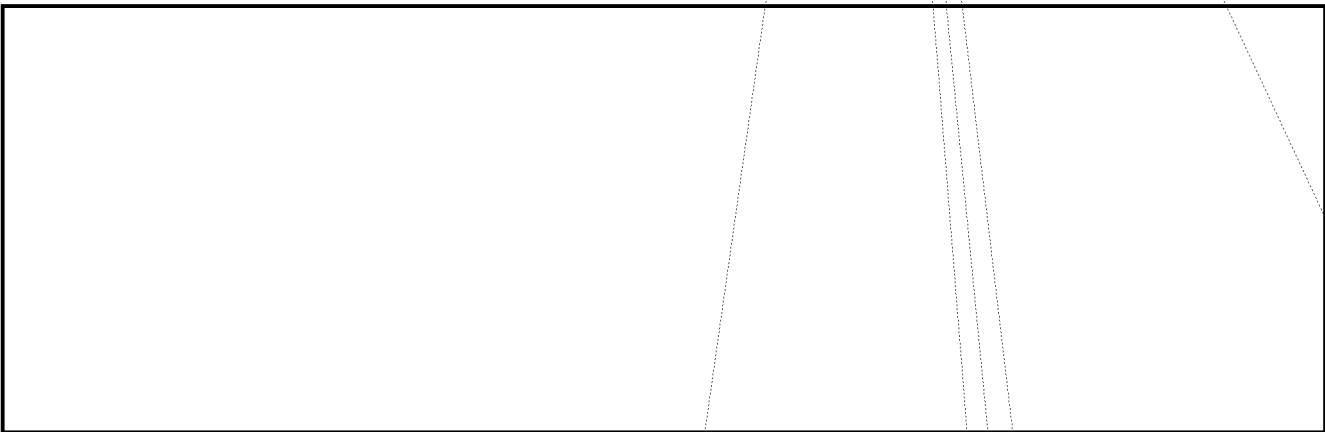
~~TOP SECRET~~

Security Information

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

by the [] are adequate; the State Department member may be in a position to certify the findings of the U. S. delegation to the Tripartite Working Group.

4. The conditions postulated by USCIB regarding an approach to the MFA have been fulfilled to some degree. Additionally, the [] cryptanalytic organization recently expressed to the [] its concern over the insecurity of the [] of NATO nations, particularly those of [] and [] and during 1952 there was a marked improvement in the behavior of the [] on cipher security matters.



6. Recommended actions:

a. If the improvement of [] general security is confirmed, USCIB agree that the conditions which deferred action on the [] communications security problems have been removed.

b. USCIB accept the method of approach to the MFA suggested by the U.K. in its letter of 10 December 1951 (Tab 8 in folder), and nominate a senior representative, together with a technical adviser, to meet with [] representatives in Paris at a specified date.

c. State Department member brief the U. S. Ambassador to [] on the proposed procedure of approach.

~~TOP SECRET~~

Security Information

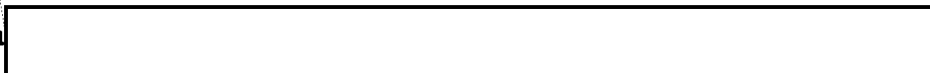
~~TOP SECRET SECURITY INFORMATION CANOE~~EO 3.3(h)(2)
PL 86-36/50 USC 3605

18 May 1953

REPORT OF AD HOC COMMITTEE ON EXAMINATION
OF TELECOMMUNICATIONS OF NATO NATIONSPROBLEM:

1. To examine the available telecommunications traffic of NATO members in order to measure (a) the incidents of violations of NATO communications security regulations; and (b) the extent of potential

SCOPE AND METHOD OF THE INVESTIGATION:

2. This Committee was established at the 82nd meeting of USCIB on 13 February 1953 to examine the problem of communications security violations by NATO members. The Committee filed a report dated 30 April 1953 which set forth certain findings pertaining to security violations detected in the available traffic and centered principally on  During the period of this initial study, arrangements were made to hold a BRUSA conference on the entire problem of NATO communications security. With that fact in mind, USCIB decided at its 84th meeting on 8 May 1953 that this Committee should continue its investigation on broader lines which would include not only a consideration of security violations but also an effort to determine the extent of potential damage to US interests resulting from leakage of

~~TOP SECRET SECURITY INFORMATION CANOE~~

EO 3.3(h)(2)

PL 86-36/50 USC 3605

-2-

[REDACTED]

communications security practices. This report covers all phases of the expanded problem.

3. The original directive called for representatives of the Departments of State and Army to coordinate with the Director, NSA in preparing a report. It soon became apparent that the investigation would touch areas in which all member departments and agencies of USCIB have an interest. Consequently, the Departments of Navy and Air Force, the Central Intelligence Agency and the Federal Bureau of Investigation were asked to participate in the survey and their representatives have joined in various phases of the investigation and the preparation of this report.

4. The results of this survey are presented in the four Tabs attached hereto. Tab A presents the investigation into security violations and is in substance the initial report presented to USCIB under date of 30 April 1953. Tab B is a statement of the situation as it pertains to military traffic. Tab C represents a substantive

[REDACTED]

Tab D represents a cryptologic evaluation of the NATO nations under consideration.

5. There is also attached a Tab E which consists of a brief



This Tab is not

a direct product of the Committee's investigation but is presented as a convenience to the members of the Board in their consideration of the entire problem.

6. Each phase of the Committee's work is subject to particular limitations which are described in the relevant attachments to the report. However, certain general restrictions in coverage were necessary to make the Committee's work manageable and are applicable to all the attachments, as follows:

(a) The traffic examined was limited to messages sent between 1 November 1952 and 1 May 1953. Although a few messages transmitted prior to 1 November 1952 are included in this report, they are items which were brought to the attention of the Committee primarily as examples of the type of material desired and their inclusion here does not mean that the period prior to 1 November 1952 was examined thoroughly.



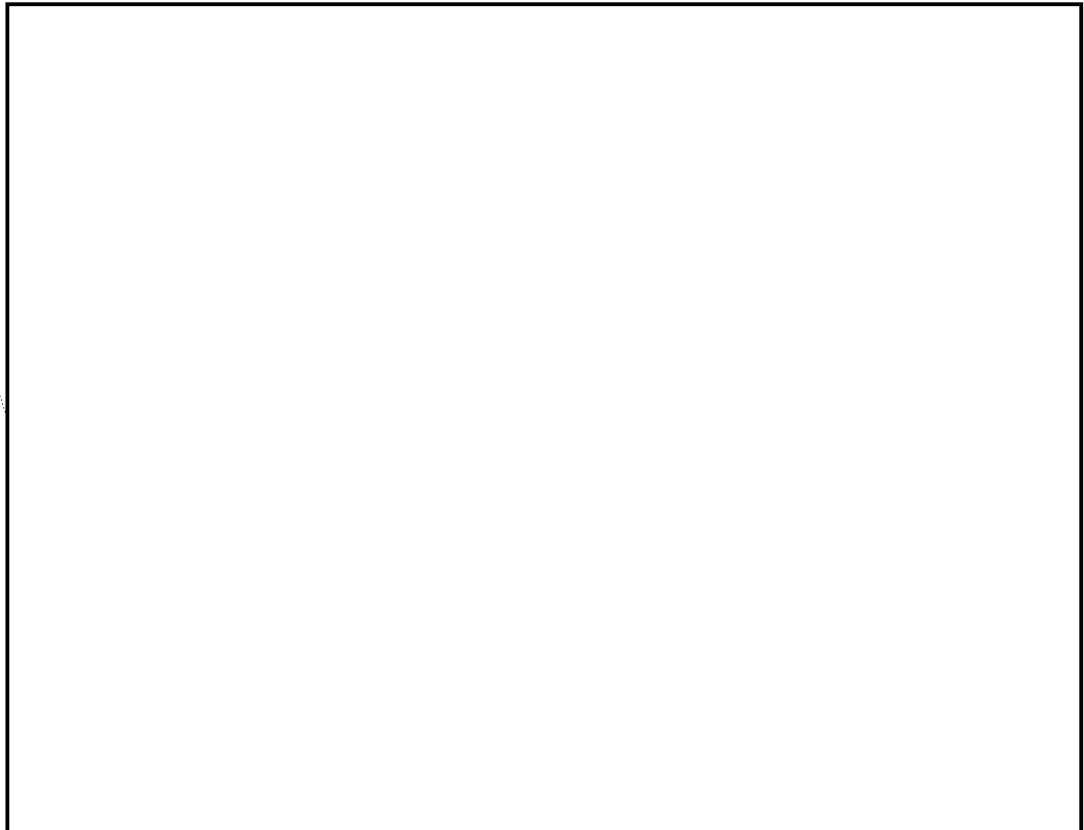
In no phase of the Committee's investigation can it be stated that all of the available traffic during this period has been examined. The Committee endeavored to cover all major circuits, and through this search and by checking the files of the departments and agencies represented on the Committee, it is estimated that an accurate total appraisal has been achieved. The inability to examine every message

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

-4-

means, of course, that some items have been overlooked. However, the Committee does not believe that the number or quality of such messages would be such as to alter the principal conclusions of this report.

7. The Committee's conclusions must be qualified by certain assumptions which were made in order to center the focus of attention on the content of the traffic and to avoid inquiries beyond the competence of the Committee. It was assumed that

~~TOP SECRET SECURITY INFORMATION GANCE~~

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

CONCLUSIONS:

A. On security violations:



UK agrees

||

||

||

|| as no

UK generally agrees

hold up around of this one

7. The proper US-UK authorities on NATO should be fully informed of the security violations with respect to NATO matters and be urged to develop a program of strict observance of NATO

~~TOP SECRET SECURITY INFORMATION CANCE~~

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

-6-

in which task
the
regulations. Initial efforts along this line should not involve



regulations
on this
we're to
agree

agree

2/1

4

pass

pass

~~TOP SECRET SECURITY INFORMATION CANOE~~

-7-

appraise, especially in hindsight. The Committee has made every effort to be accurate as well as objective in examining this traffic but the number of examples found in this survey cannot be presented as an absolute figure. Nevertheless, when one takes into account the huge number of messages examined by all the evaluating agencies in the course of their normal operations during the test period chosen for this survey, and the intensive effort on the part of the representatives of these agencies meeting in committee to identify examples of information leakage injurious to US interests, it is evident that the leakage, insofar as quantity is concerned, is very small.

6. Despite the quantitative insignificance of the foregoing examples,

[Redacted]

This survey has brought out a reasonably comforting fact in the sense that few damaging examples were uncovered, but this must be balanced against the possibility that at any moment critically damaging information could appear in the same type of traffic. The latter aspect of the situation is covered in the section immediately following.

*Part to
out*

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

D.

*agree
OK*

*Limited to
Diplomats*

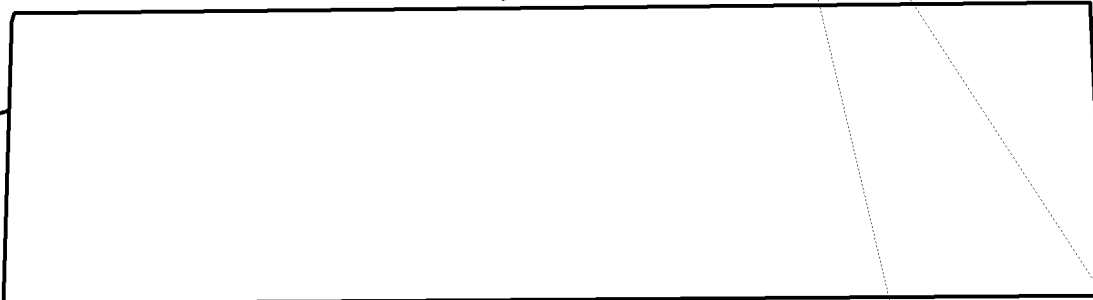
agree

agree

agree

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~



agree

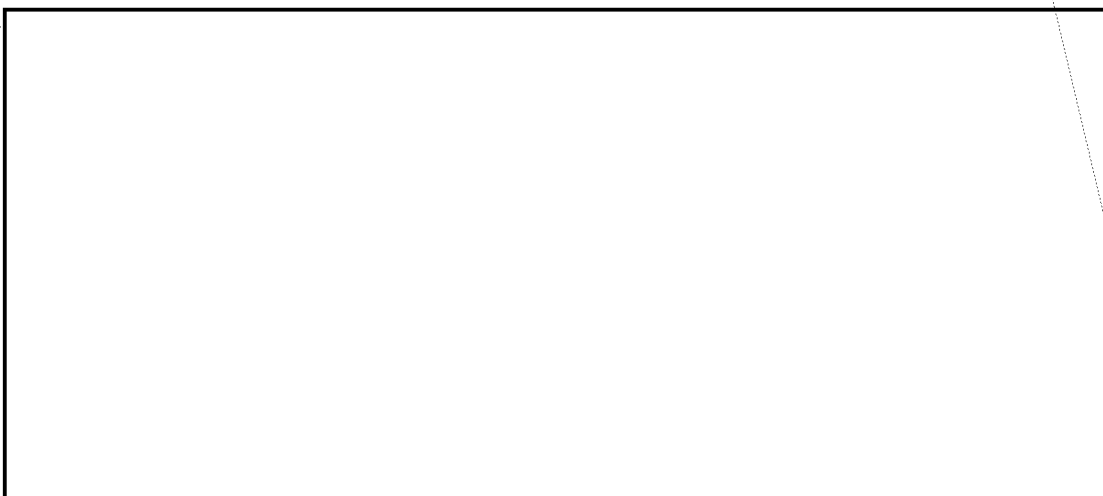
*out of line
with new
recs*

Labor

7. An effort to improve national cryptographic and communications practices could reduce appreciably the total communications security problem under consideration and should be made prior to any effort to improve systems or to encourage the use of more complicated cryptographic equipment.

8. A substantial improvement in the general situation might result from the institution of a security demonstration among the NATO countries.

E. Other conclusions:



Intell Com

agree

3. The evidence brought out in this investigation does not indicate that serious damage has occurred during the period covered by this survey. However, such damage has occurred in the past and may occur again in the future.

*Int
Com*

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

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



Agree

RECOMMENDATIONS:

1. The US-UK authorities in NATO should be fully informed of the security violations with respect to NATO matters for the purpose of developing a program of strict observance of the NATO communications security regulations.

Agree

2. An effort should be undertaken jointly with the British to improve the national cryptographic and communications practices of the NATO countries by a demonstration of proper techniques, explanation of [redacted] and other means short of direct [redacted] at this time. Such demonstrations and explanations must be considerably detailed even to a point that might be expected to permit reasonable suppositions as to [redacted]

Agree

3. Machinery should be established jointly with the [redacted] for the continuing examination of the traffic of NATO countries and for the analysis of their communications practices in order to supplement this survey, to judge the effect of the efforts to improve their security and to provide a basis for future action.

Agree

~~TOP SECRET SECURITY INFORMATION CANOE~~

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

1. This phase of the Committee's investigation of traffic was undertaken prior to and separately from the investigation covered by Tabs B and C and is limited to a consideration of security violations. For the purpose of this report the Committee defined a security violation as any message violating NATO communications security regulations. The definition was adopted because those regulations constitute the only standard agreed upon by the NATO countries.

"COSMIC. The word COSMIC has been designed as a security warning only. This designation shall, in addition to the appropriate security classification, be placed on all joint and national papers tabled at meetings of any body or committee set up under the North Atlantic Treaty Organization which contain and reveal:

- (1) Strategic or operational military appreciations, plans or decisions.
- (2) Political-military appreciations, plans or decisions.
- (3) Economic planning based on strategic military plans and decisions which could lead to disclosure of such plans and decisions.
- (4) Classified information of one country tabled or circulated by another country, unless the 'owner' country agrees otherwise.

TAB A~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

"NATO. On all other joint or national documents tabled or circulated within the North Atlantic Treaty Organization the word "NATO" shall appear, together with the appropriate security classification. This "NATO" marking, however, does not require the special handling or accounting provided for "COSMIC" documents, other than as warranted by the security classification, and no special screening (as required for "COSMIC" personnel) is necessary for access to NATO documents."

3. The investigation of security violations was subject to the assumptions described in paragraph 7 of the report and to the time limits described in paragraph 6. It did not cover the traffic of

[redacted] but was concentrated on the [redacted]

[redacted] came to the

attention of the Committee, but the traffic of those countries was not examined in detail.

4. In examining traffic for security violations the Committee considered 119 individual messages which were submitted primarily by

[redacted] The Committee screened this list

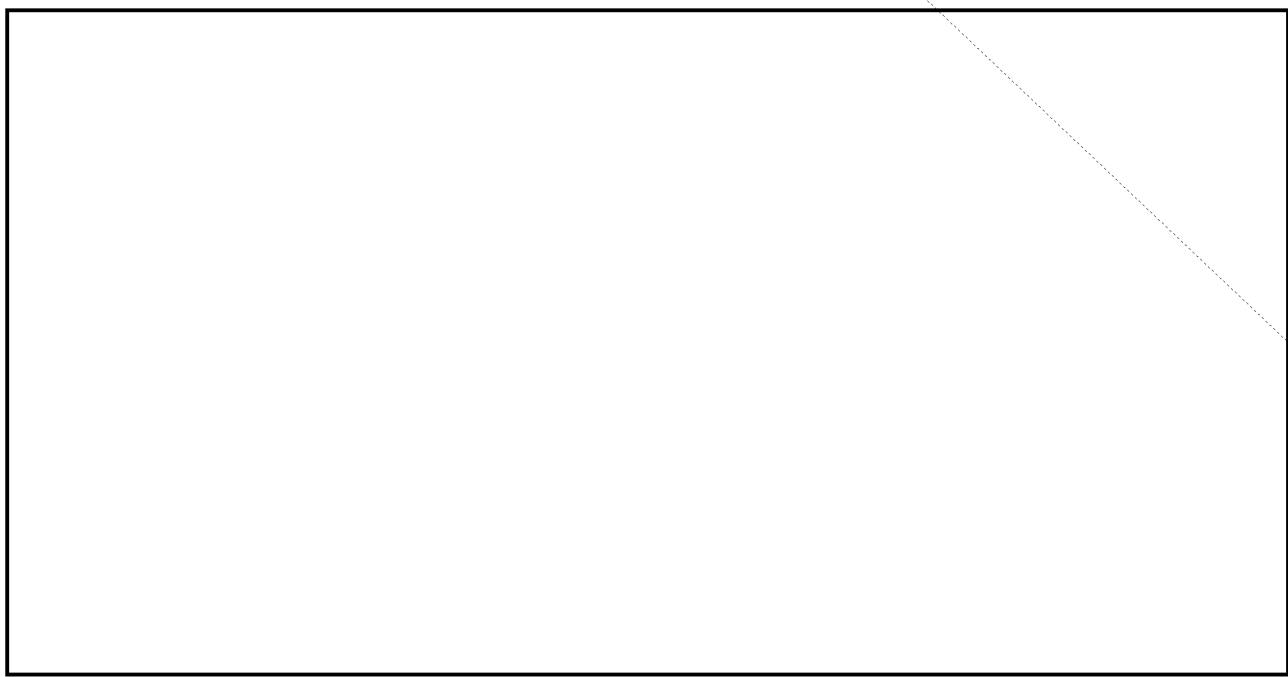
to eliminate messages which clearly did not constitute security violations.

5. In the course of this phase of the investigation the Committee encountered certain messages which contained information damaging to the

~~TOP SECRET SECURITY INFORMATION CANOE~~

TAB A

~~TOP SECRET SECURITY INFORMATION CANOE~~



~~TOP SECRET SECURITY INFORMATION CANOE~~

TAB A

~~TOP SECRET SECURITY INFORMATION CANOE~~

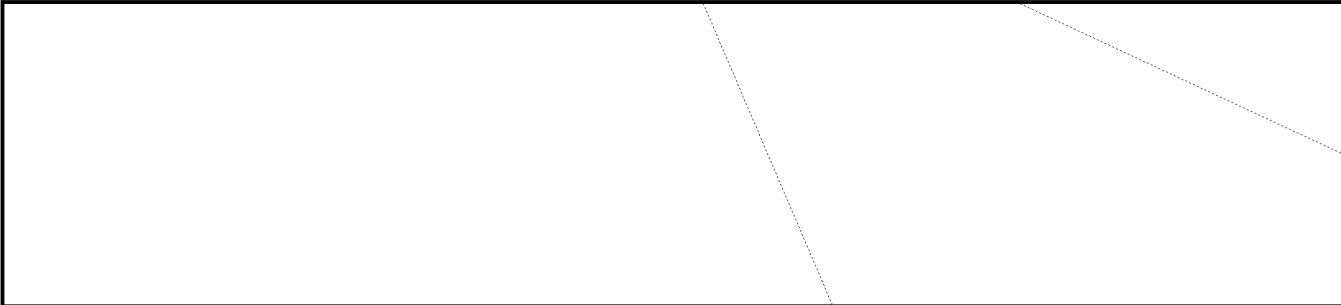


4. Therefore, no categorical statement can be made to the effect that there has been or has not been any "leakage" to the USSR of information damaging to US interests.

TAB B

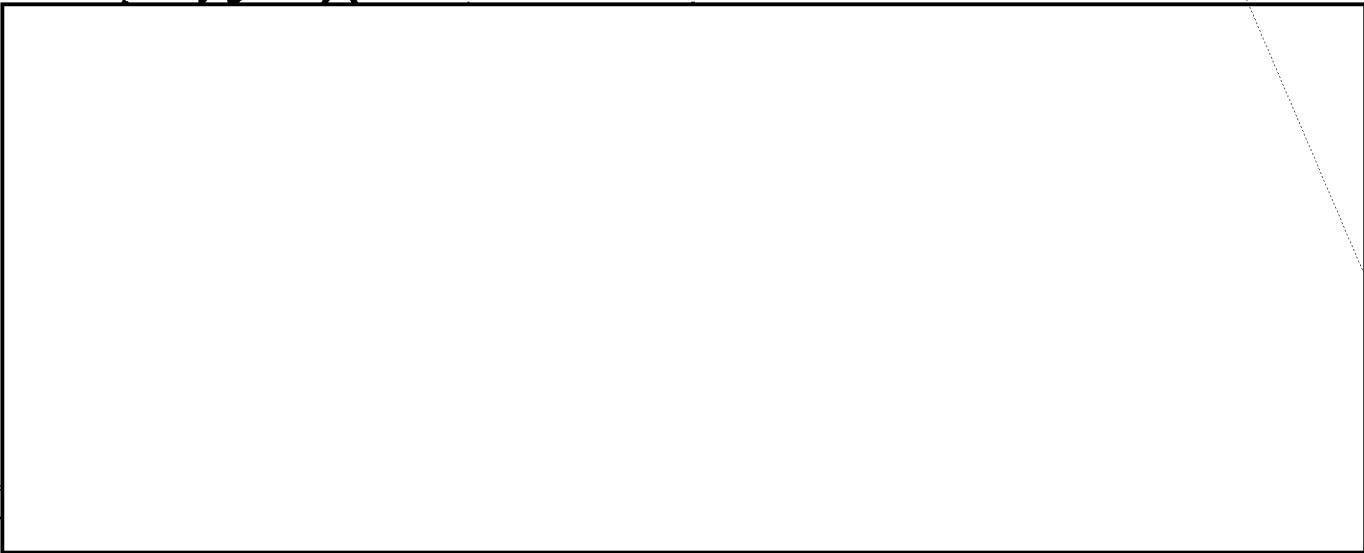
~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~



compromise might be injurious to US interests. A message was considered to affect US interests if it related to matters in which the US was taking action or to a policy which the US was supporting. A message was considered damaging if the USSR could use the information either on a long or short term basis to thwart or hamper action taken by the US or the policies supported by it. Messages containing information affecting US interests were not considered damaging if timely information were available to the USSR through open sources such as newspapers or public release of government information.

2. The material studied during this phase of the investigation falls into the following categories:



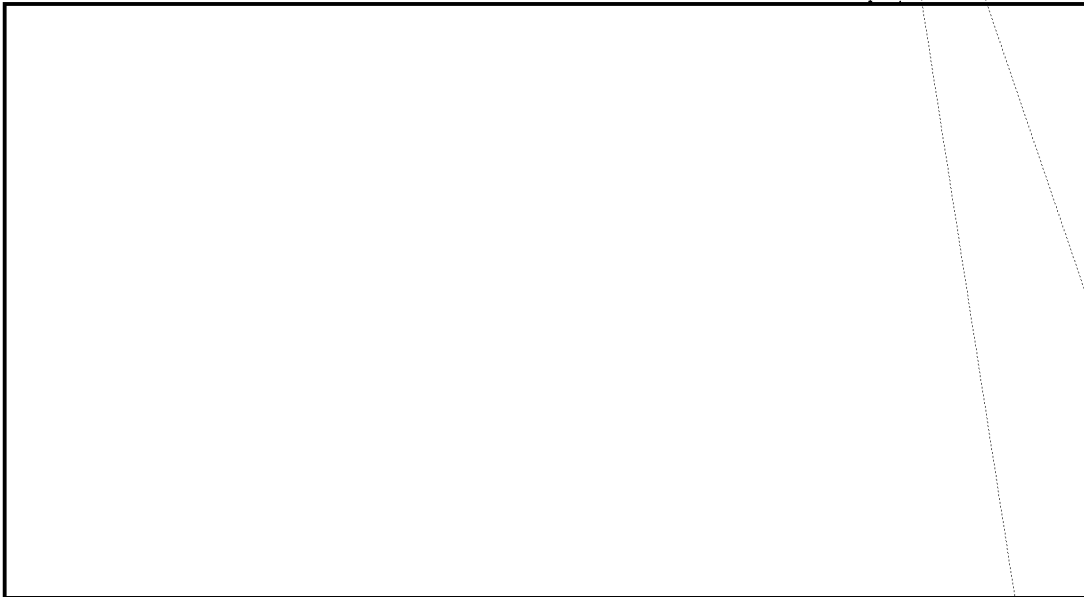
Phy 11/15

~~TOP SECRET SECURITY INFORMATION CANOE~~

TAB C

~~TOP SECRET SECURITY INFORMATION CANOE~~

of this report⁷ were checked by the Committee under the terms of reference mentioned in Paragraph 1 above.



3. On the basis of investigating the four categories noted in the paragraph immediately preceding, the Committee accepted the evaluations of the various specialist panels to the effect that

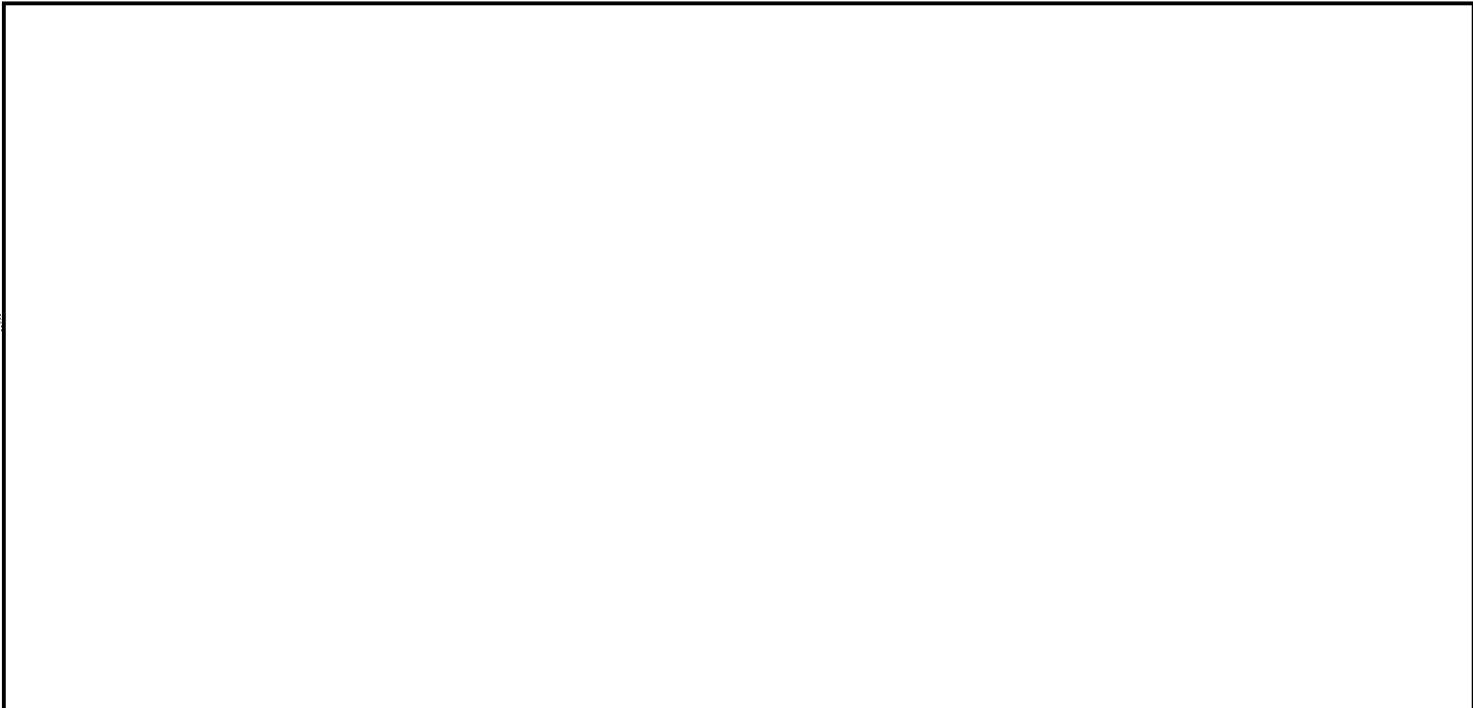


~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET CANOE~~

SECURITY INFORMATION

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



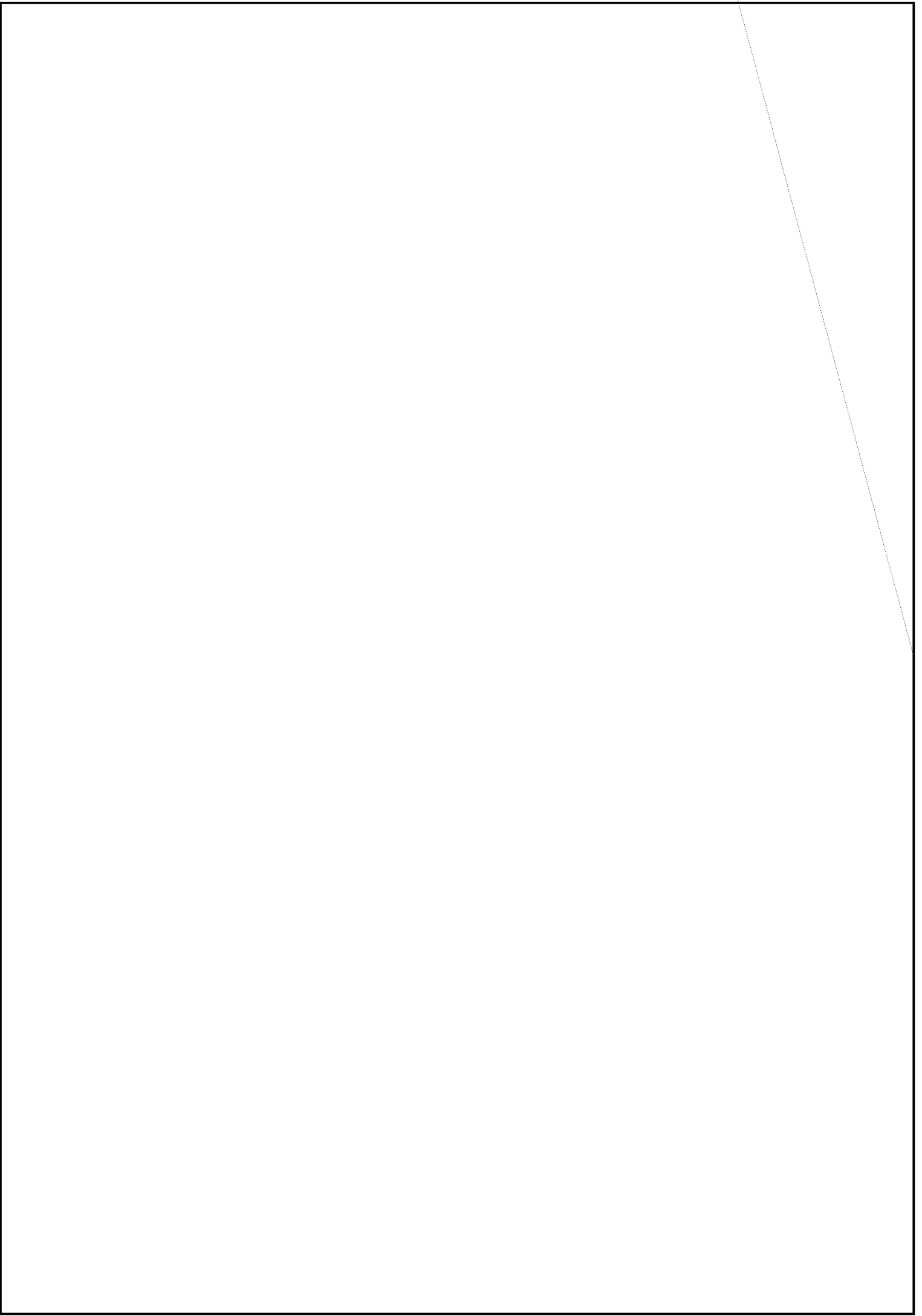
Some general remarks on each country are here prefaced to the tabulations:



SECURITY INFORMATION

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



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

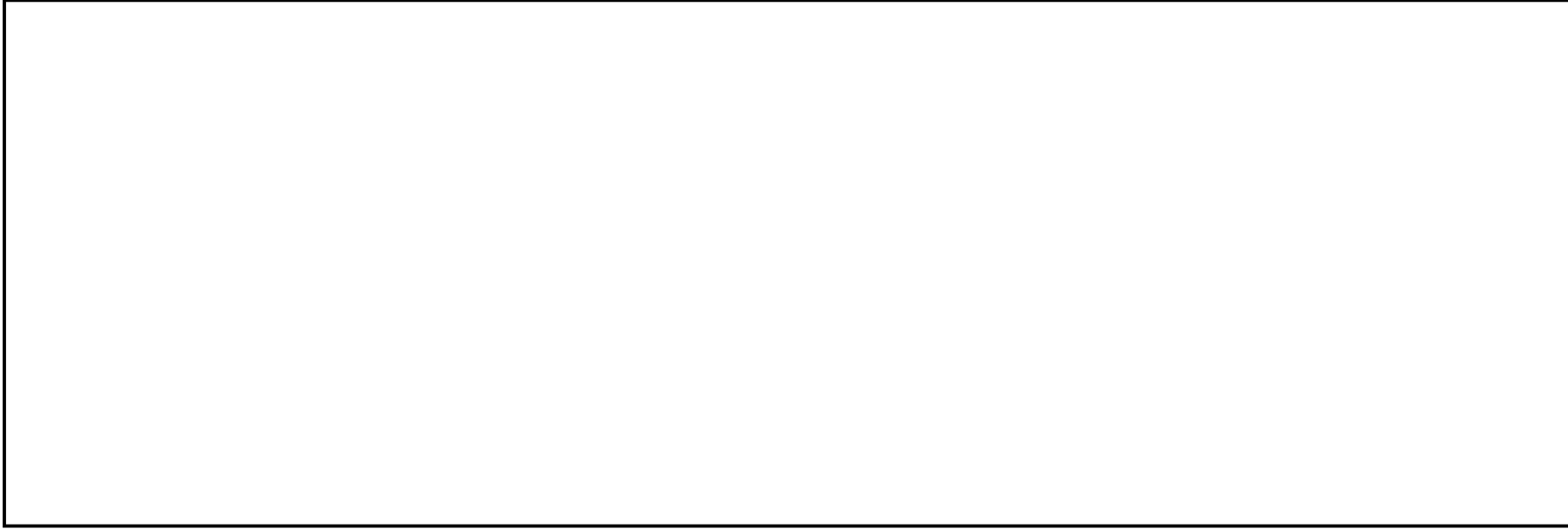
~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

- (1)
- (2)
- (3)
- (4)
- (5)



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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

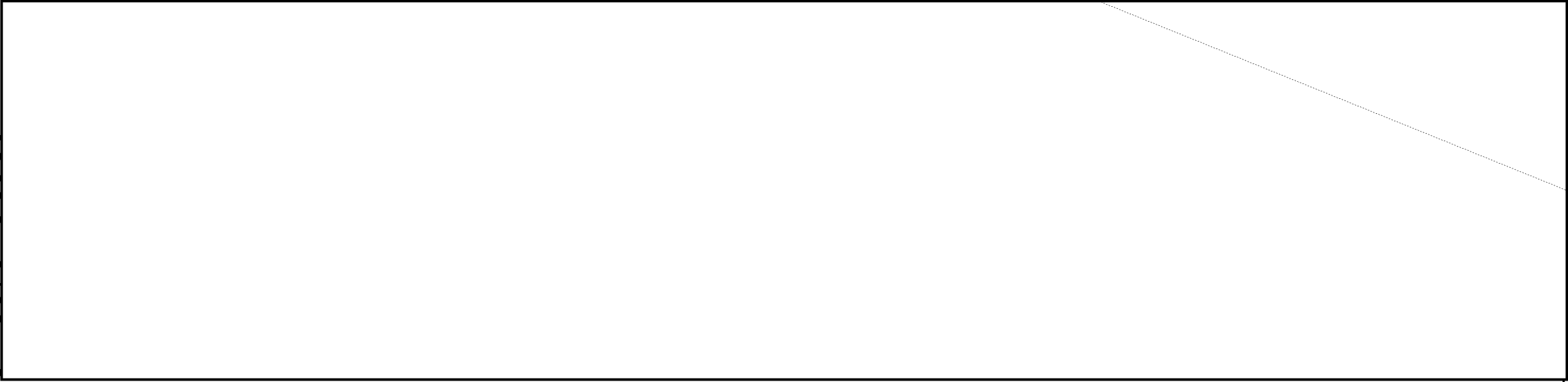
~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



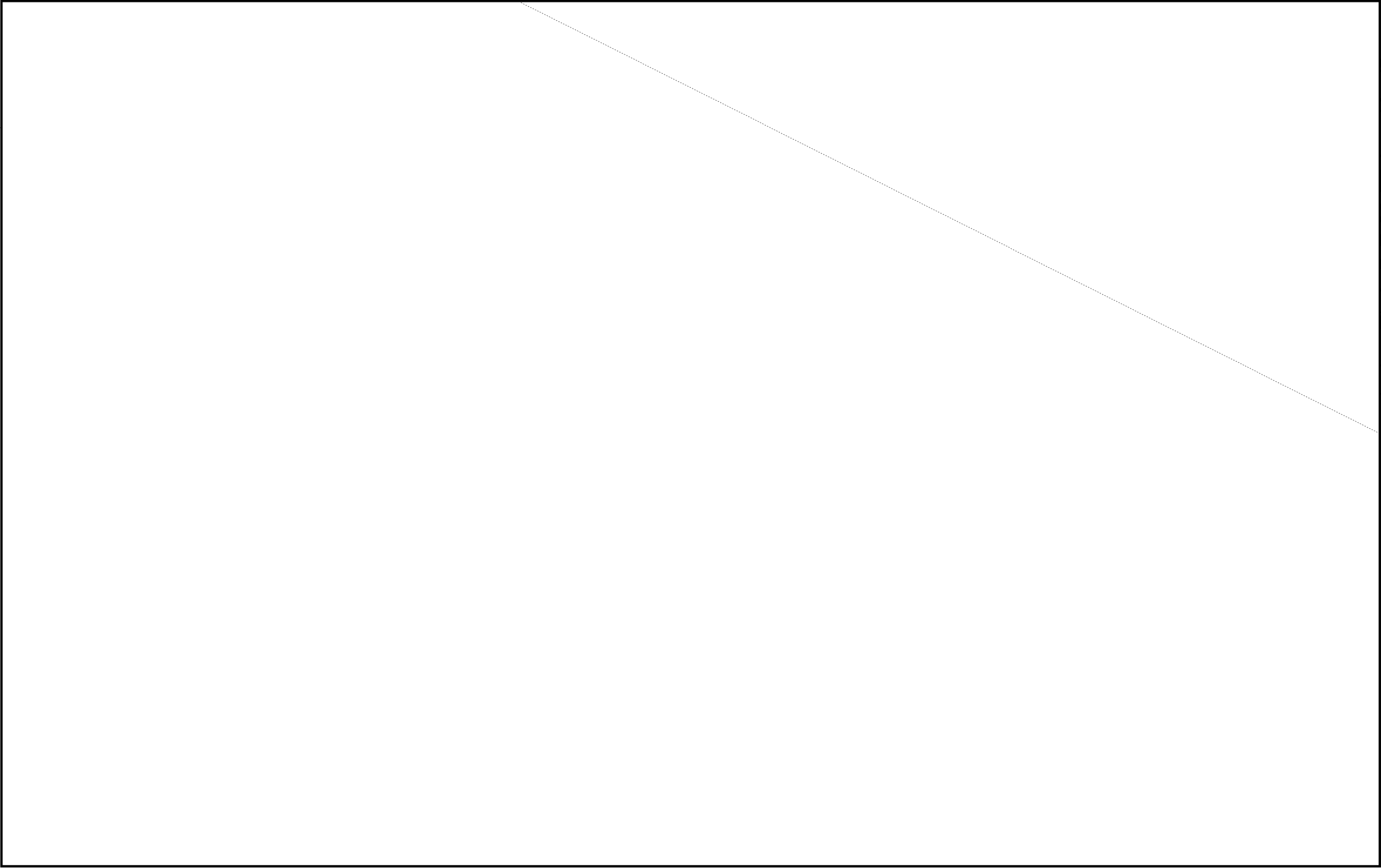
58

UNED

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

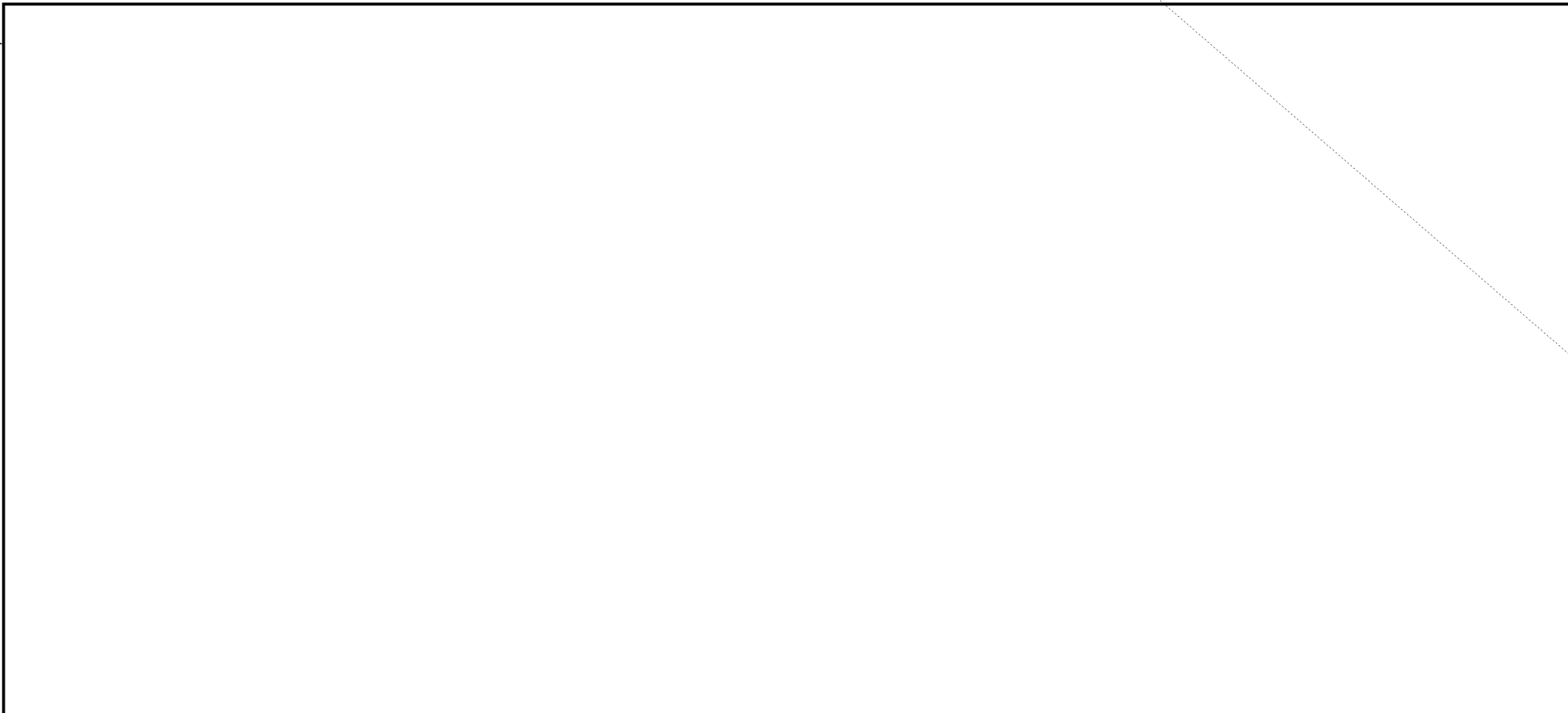
EO 3.3(h)(2)
REF ID: A6157796 3605



ACCESS
ON
OBTAIN

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



0366
a

~~TOP SECRET CANOE~~

REF ID:A517796

EO 3.3(h)(2)

PL 86-36/50 USC 3605

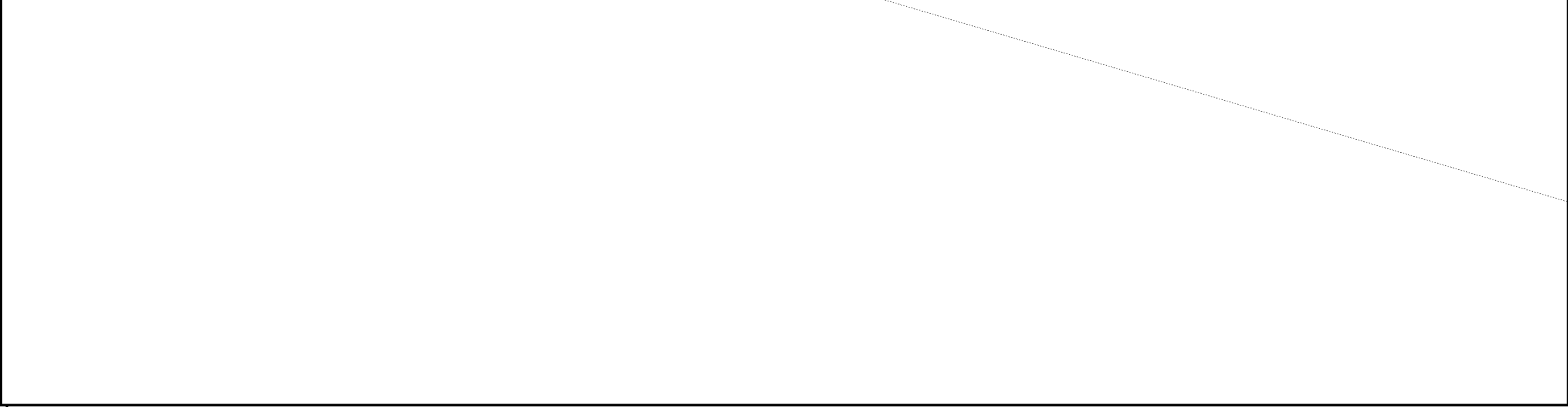
~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

EO 3.3(h)(2)
REF ID: A517796
PL 86-36/50 USC 3605



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

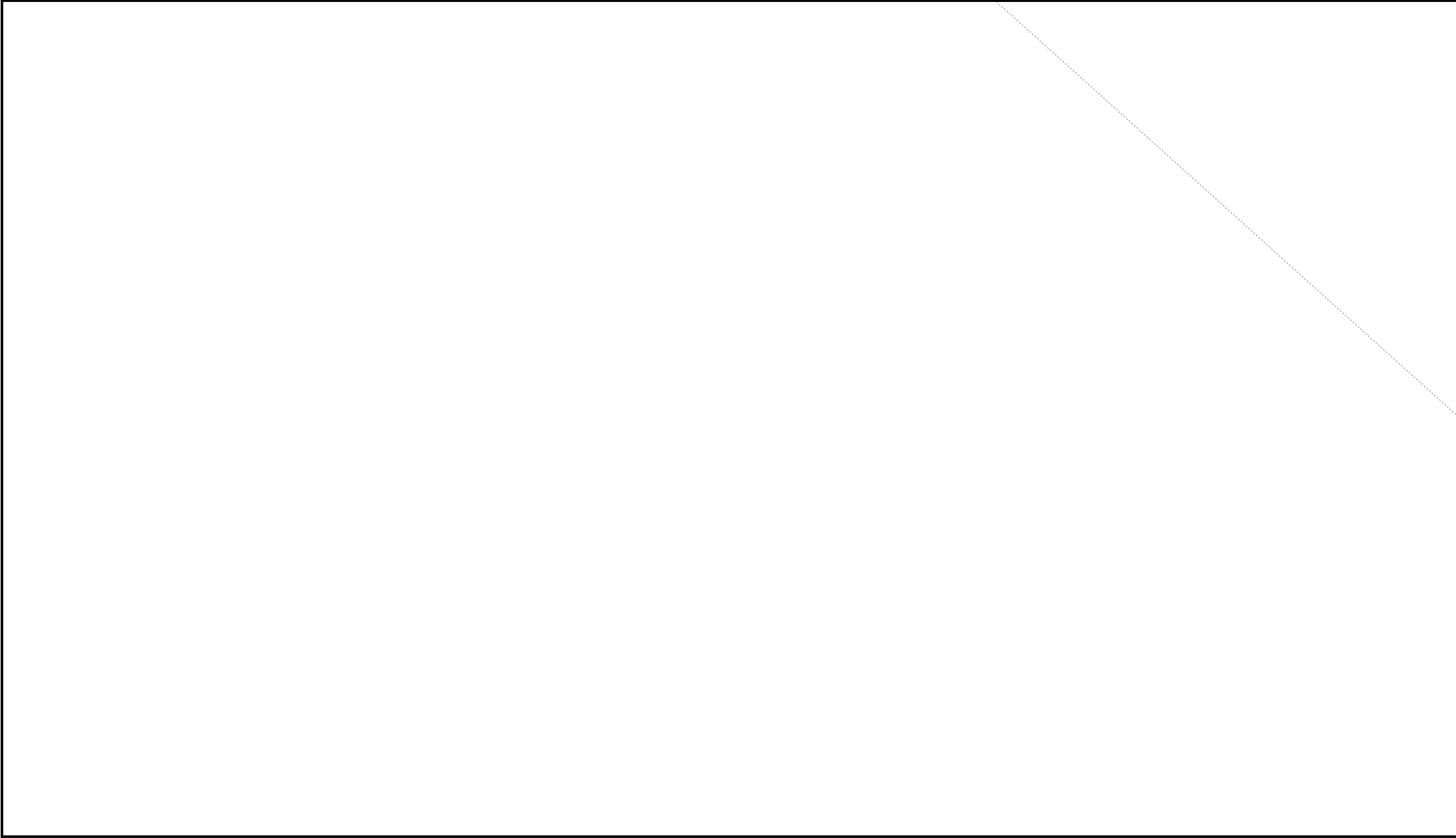
~~TOP SECRET CANOE~~

ss
ned

~~TOP SECRET CANOE~~

File

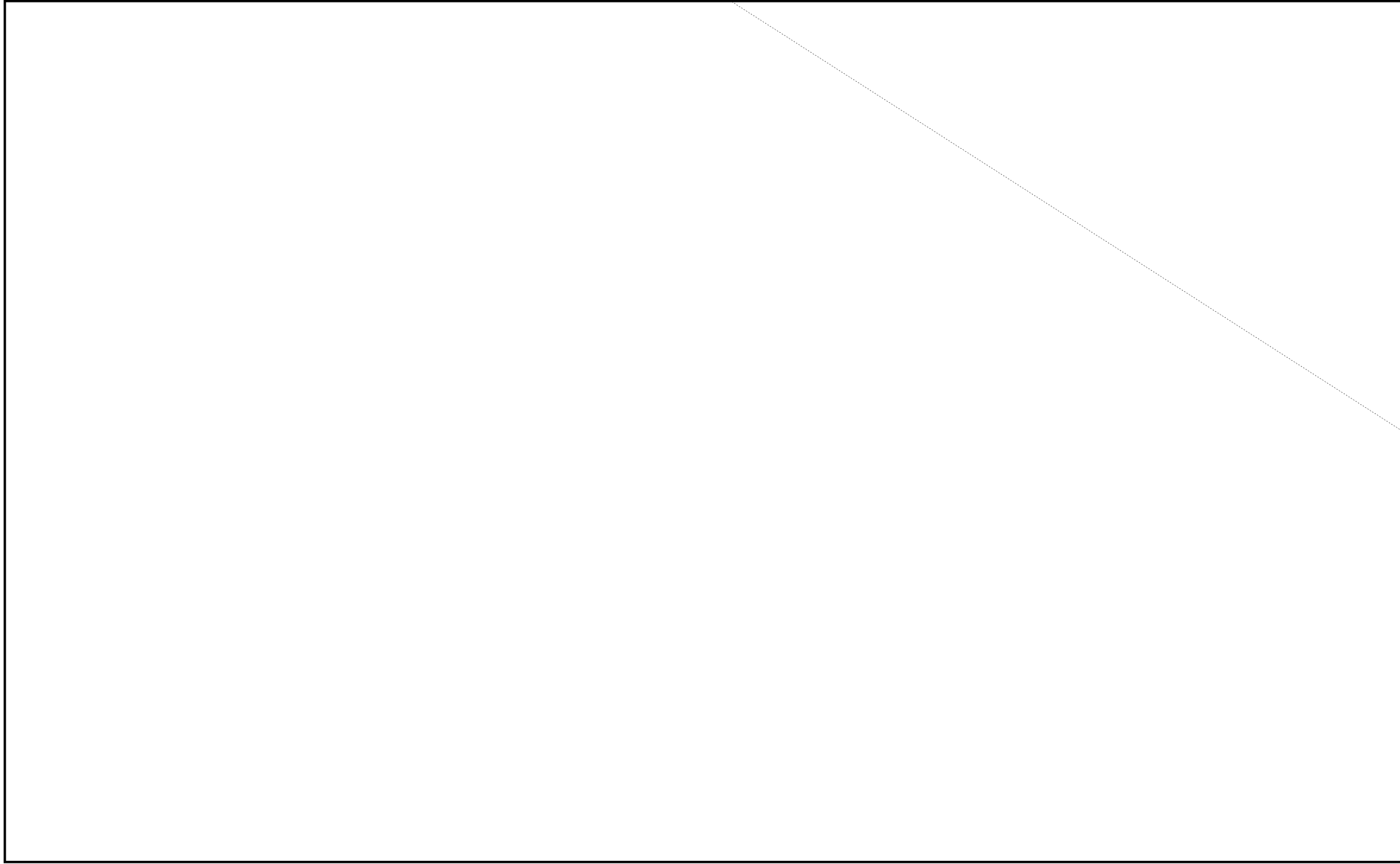
~~TOP SECRET CANOE~~



epen-
bb-

~~TOP SECRET CANOE~~

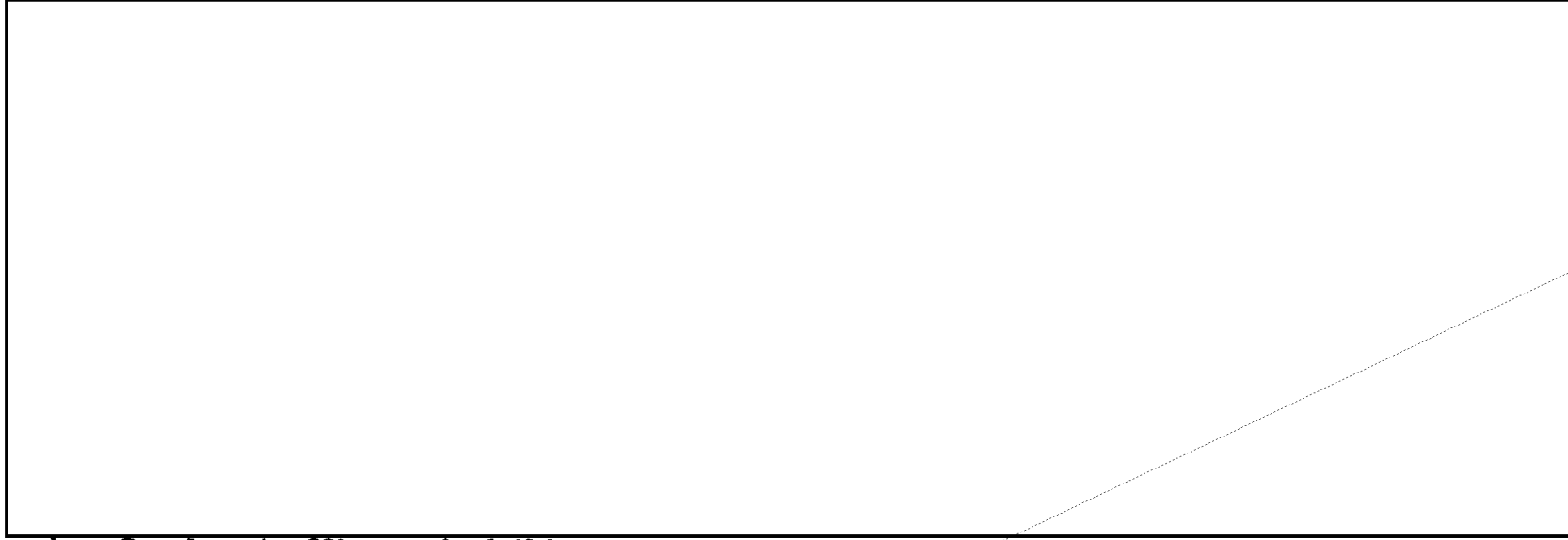
~~TOP SECRET CANOE~~



CLASS
OR

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



4. Based on traffic received this year.

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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

REF ID: ^{EQ 33(h)(2)}~~A517796~~
PL 86-36/50 USC 3605



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

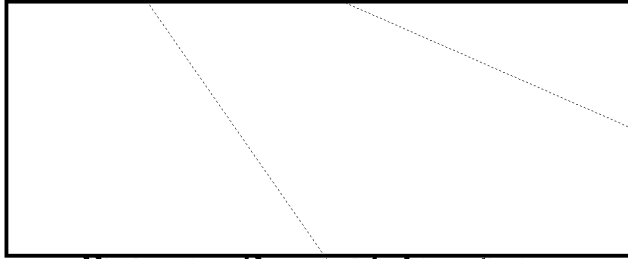
~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

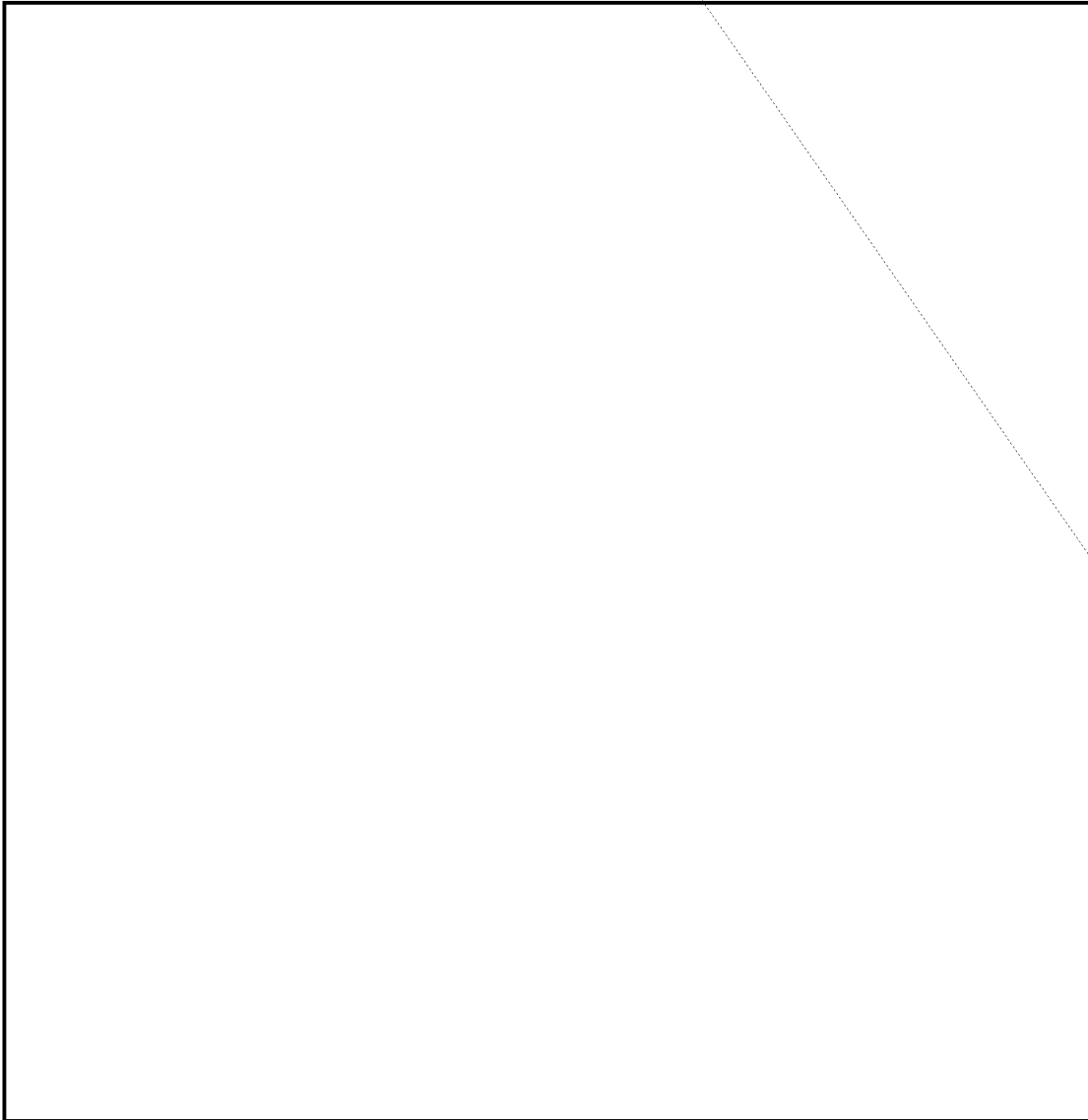


~~TOP SECRET CANOE~~

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



these are the countries whose
communications security has
been considered or dealt with
by USCIB.



problem at the request of Secretary Marshall, but was unable to

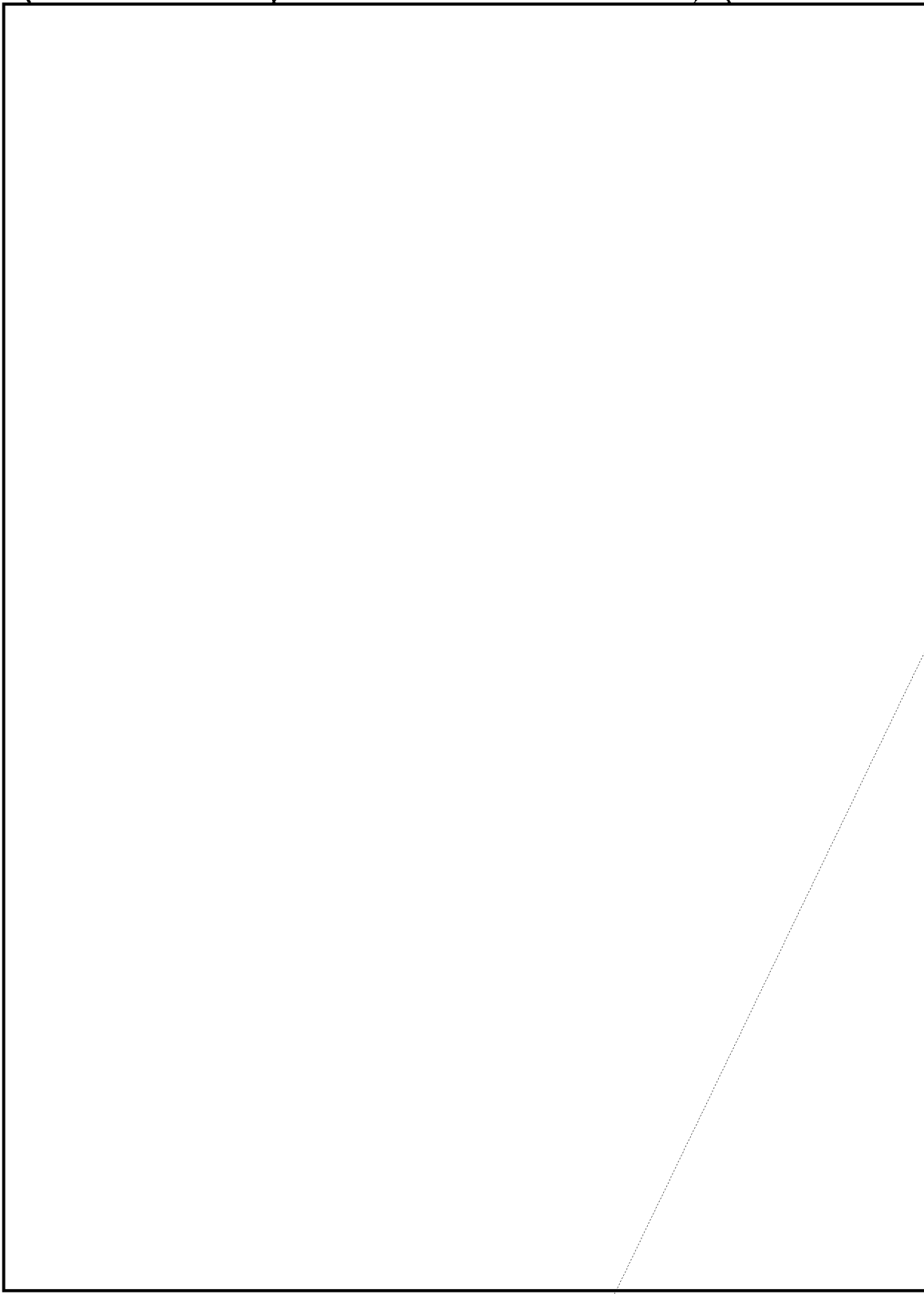
reach agreement whether the US should provide cryptographic assist-

[REDACTED]

report to the NSC on 31 August 1948 and on 2 September the NSC accepted the majority view in USCIB that these steps should not be taken. Secretary Marshall replied personally to Foreign Minister Bevin informing him of this decision.

2. A year later, in September and October of 1949, USCIB, acting on behalf of the US Government, accepted a British proposal that a British cryptographic device (the Typex Mark II) be provided to the Western Union powers, and subsequently to all NATO governments, for the exclusive encipherment of METRIC and COSMIC telecommunications. This device was subsequently adopted by NATO for this purpose.

3. During the following summer of 1950 the British Ambassador in Washington raised with the Department of State the general problem



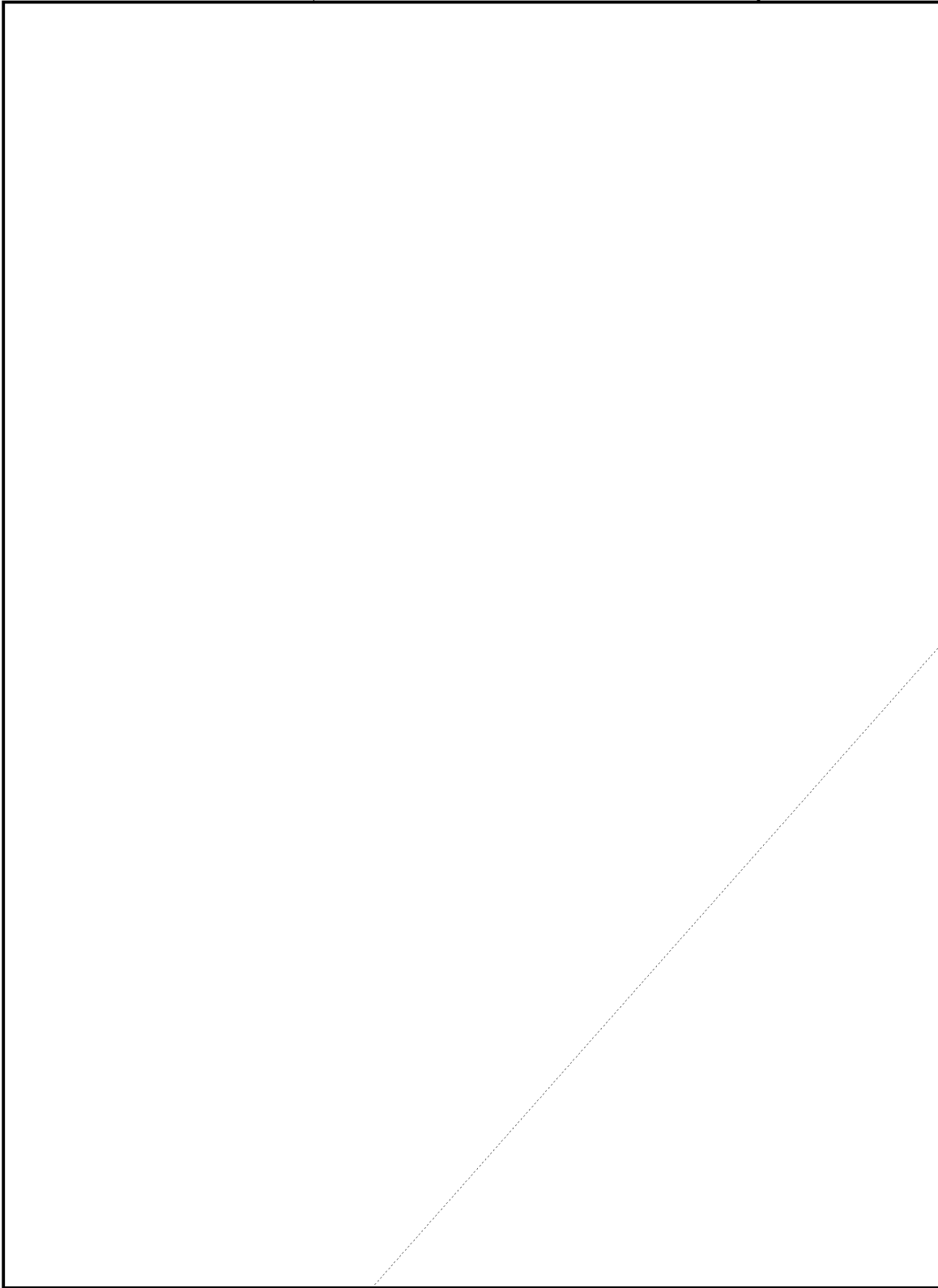
~~TOP SECRET SECURITY INFORMATION CANOE~~

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

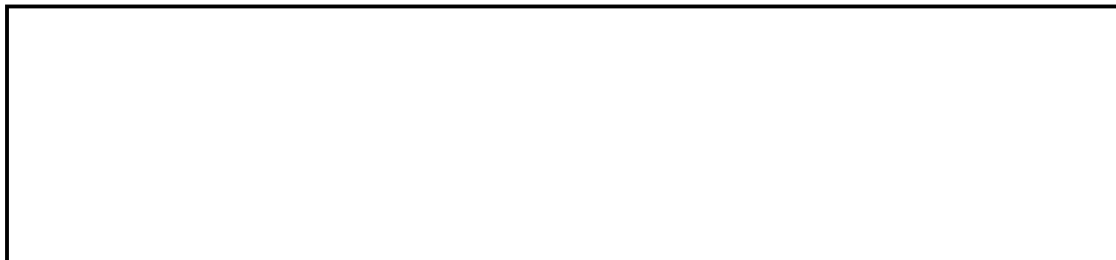


~~TOP SECRET SECURITY INFORMATION CANCE~~

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



steps to this end without awaiting either the establishment of "secure

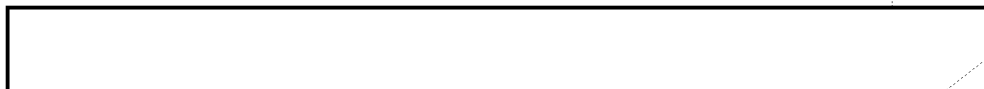


communications organizations and designed to assure adequate guarantees of security at each step of the approach. This Department of State proposal was considered by the Board at its meeting of 9 March and was withdrawn by the State member in the face of a majority view that the Board should adhere to the more rigid policy which it had already adopted. The specific proposals for the scope and agenda for the forthcoming conference were approved, however, and were forwarded to LSIB on 13 March 1951 (14/128).

8. The BRUSA Conference was held in May 1951 and its Report (14/132) was submitted to USCIB on 15 May. USCIB approved the Report at its meeting on 24 May and decided also to refer it to the NSC for approval and to perpetuate the US conference delegation as an Ad Hoc Committee of the Board to keep this problem under continuous review. LSIB notified us of its approval of the Report by letter of 7 June 1951 (13/188). The Report was forwarded to the NSC on 8 June 1951 (14/137) and was approved by the Special Committee of the NSC and the President on 11 January 1952 (14/189).

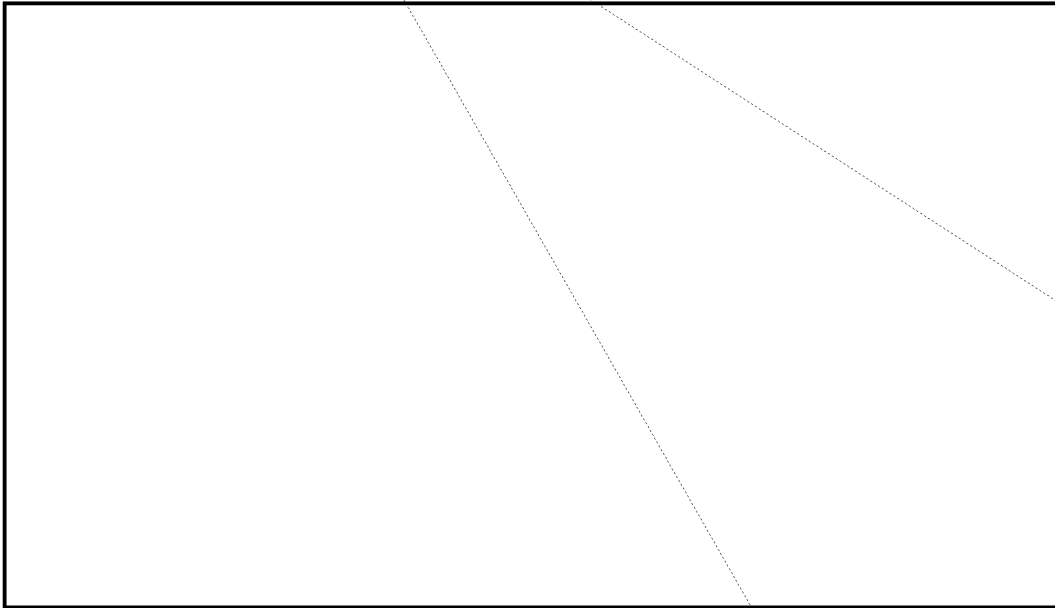
9. The principal results of this BRUSA Conference were:

- (a) The preparation of a specific cryptographic plan which could accomplish the desired improvement in the security



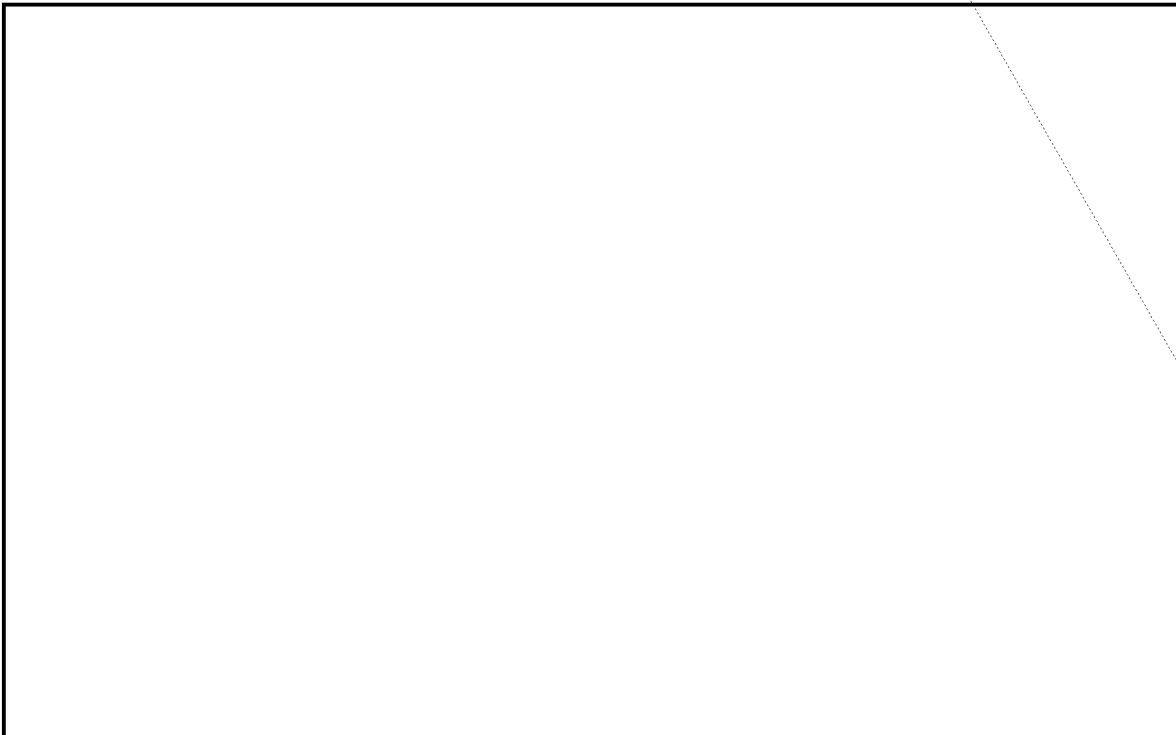
~~TOP SECRET SECURITY INFORMATION CONF~~

7.

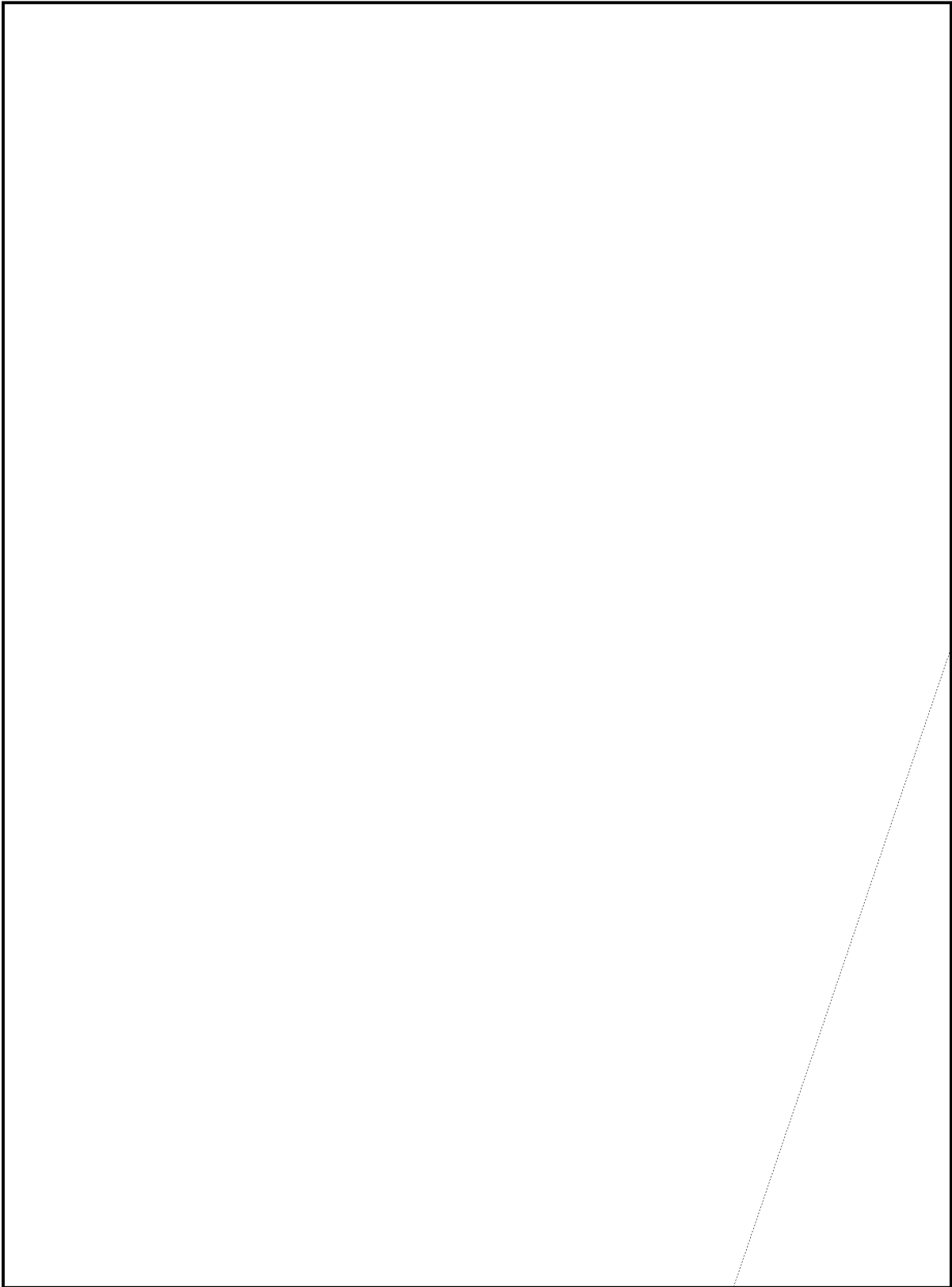


- (d) The establishment of general security conditions or criteria which must be met to the satisfaction of both LSIB and USCIB prior to taking action.

It may be noted that the work of this Conference was based on a prior assumption that the need to take direct action to improve the security

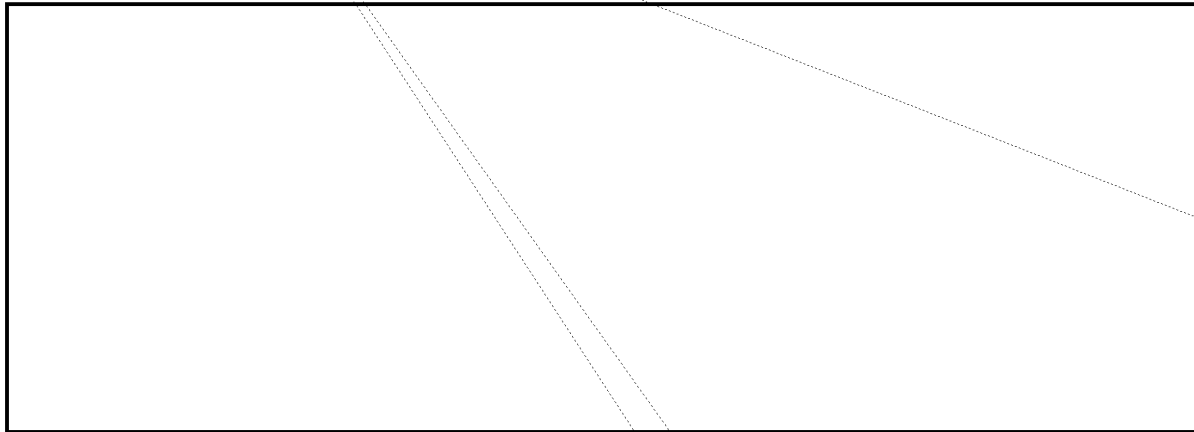


~~TOP SECRET SECURITY INFORMATION CONF~~

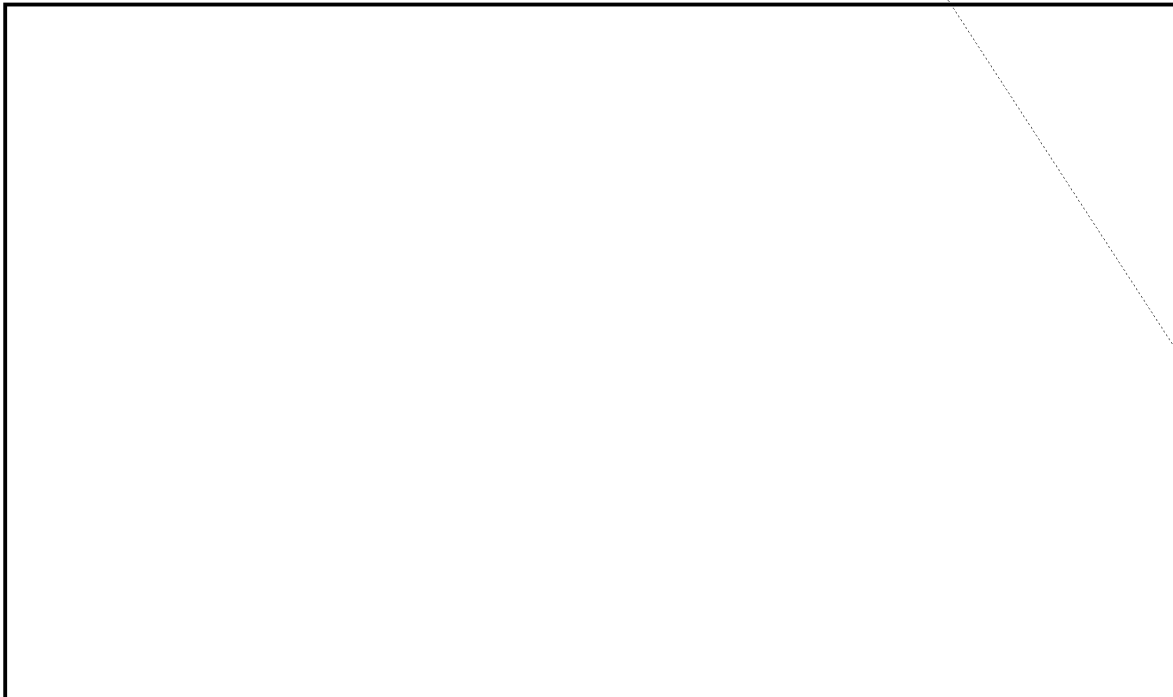


~~TOP SECRET SECURITY INFORMATION CANOE~~

9.



security should not be made until the Report had been approved by each of the participating countries and the [] had taken definite action on the basis of the Report. The Ad Hoc Committee was ordered to study the specific plan proposed by the British. These views were communicated to LSIB in a letter of 24 January 1952 (14/196). The Ad Hoc Committee rendered its report on 13 February 1952 (14/200) in which it endorsed the reply which USCIB had made to LSIB and recommended further that no approach should be made until another

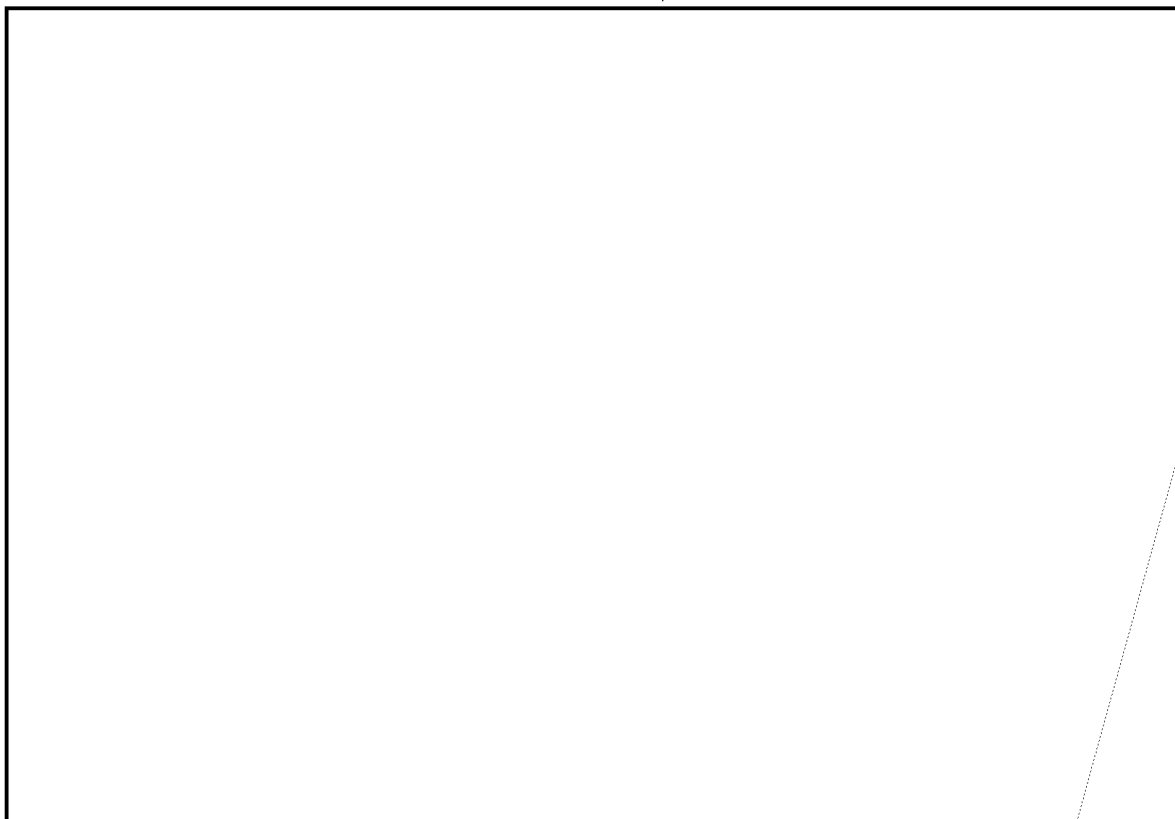


~~TOP SECRET SECURITY INFORMATION CANOE~~

the Department of State in which the British suggested that Secretary Acheson might be prepared to endorse immediately direct action and that USCIB might, therefore, reverse its decision of the preceding January. In a message of 27 June 1952 Mr. Armstrong advised Mr. Jones that the US position in this matter had not been changed.



14. The next and latest British effort to obtain our agreement that



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

~~TOP SECRET SECURITY INFORMATION CANOE~~

11.

USCIB has advised LSIB that it has agreed to such a conference, now scheduled to commence in Washington on 4 June 1953.

15. In preparation for this conference USCIB reconsidered the general problem of the insecurity of the communications of NATO countries at its meeting of 13 February 1953 and established a new Ad Hoc Committee to review the risk to the security of US classified information created by violations of NATO communications security practices and by the insecurity of the national communications of NATO countries. A report was submitted by this Ad Hoc Committee on 4 May 1953 (23/51) and was discussed by the Board at its meeting of 8 May 1952. This Report dealt principally with violations of NATO communications security practices. USCIB (a) noted the initial report by the Ad Hoc Committee and decided that the Committee should continue its study of the additional phases of the problem as outlined by [redacted] with a view to submitting a report for the consideration of the Board at a special meeting to be held in advance of the 4 June BRUSA Conference; (b) agreed to defer consideration of a presentation of this entire problem to NSC until the Ad Hoc Committee Report had been reviewed.

PL 86-36/50 USC 3605

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANCEL~~

12.

EO 3.3(h)(2)

PL 86-36/50 USC 3605

COMMUNICATIONS SECURITY

16. The problem of risk to the security of the United States created by the [redacted] communications was first considered by USCIB in the summer of 1951 shortly after the BRUSA Conference on [redacted] communications security. The matter was raised by the [redacted] member at the meeting of USCIB on 22 June 1951 in connection with several

[redacted]

of the express request of the US originators of the information.

USCIB directed that the Ad Hoc Committee, composed of members of the American Delegation to the recent BRUSA Conference on [redacted] communications security, study and evaluate the problem of [redacted] communications security.

17. The first Report of this Ad Hoc Committee (23/18) was submitted to USCIB at its meeting on 13 July 1951 and was accepted. USCIB directed that the Committee continue its study with particular regard to the problem of correcting [redacted] abuse of NATO communications security procedures. In this first Report the Ad Hoc Committee had concluded that:

- (a) [redacted] but
that on the whole, so far as NATO or US political and

~~TOP SECRET SECURITY INFORMATION CANCEL~~

~~TOP SECRET SECURITY INFORMATION CANCE~~

13.

economic policy was concerned, the information disclosed through insecure [] communications was not highly detrimental to the security of the US.

- (b) The level of [] was so low as to afford little likelihood that an improvement in their communications security would effectively prevent leakage of information affecting the security of the US.
- (c) There was no assurance that all available authorized means within the NATO organization have been applied toward the correction of [] abuse of NATO communications security procedures.
- (d) Direct action toward the improvement of over-all [] communications security was, therefore, not justified at that time.

The Ad Hoc Committee had recommended that their study be continued and that no direct action vis-a-vis the [] be contemplated until USCIB or the NSC had decided whether such action should be taken vis-a-vis the []

18. The final Report of the Ad Hoc Committee (23/22) was submitted on 7 August 1951 and was considered by USCIB at its meeting on 10 August. In this Report the Committee re-affirmed its previous recommendation that no direct action should be taken at that time beyond an effort to correct [] abuse of NATO communications

~~TOP SECRET SECURITY INFORMATION CANCE~~

~~TOP SECRET SECURITY INFORMATION CANCEL~~

14.

security procedures. The Committee recommended both a plan for an immediate approach to the [] to this end and several long-range proposals directed toward eventual over-all improvement of [] communications security.

- (a) The plan for immediate action envisaged a unilateral US approach to the [] at the ambassadorial level wherein we would advise the [] that we had been apprised of a [] violation of NATO communications security procedures and would request categorical assurance that they would correct this abuse. It was proposed also that we would offer our assurances as to the security of the NATO crypto-system (Typex Mark II) and communications procedures and that we would offer such technical assistance or advice as the [] might desire to assure themselves along these lines. This approach was to be based on the content and handling of a

[]
 on 6 July 1951; our possession of this information being attributed to an agent report [] activity. USCIB approved the recommendations of the Ad Hoc Committee and designated the State Department and CIA to develop the particulars of this approach.

- (b) USCIB has taken no action on the long-range proposals.

~~TOP SECRET SECURITY INFORMATION CANCEL~~

~~TOP SECRET SECURITY INFORMATION CANCE~~

15.

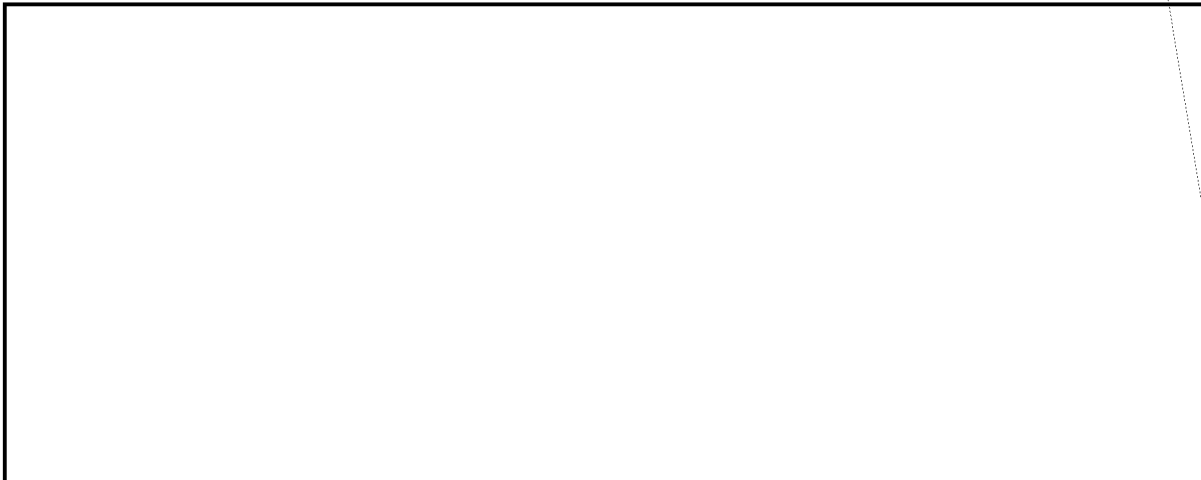
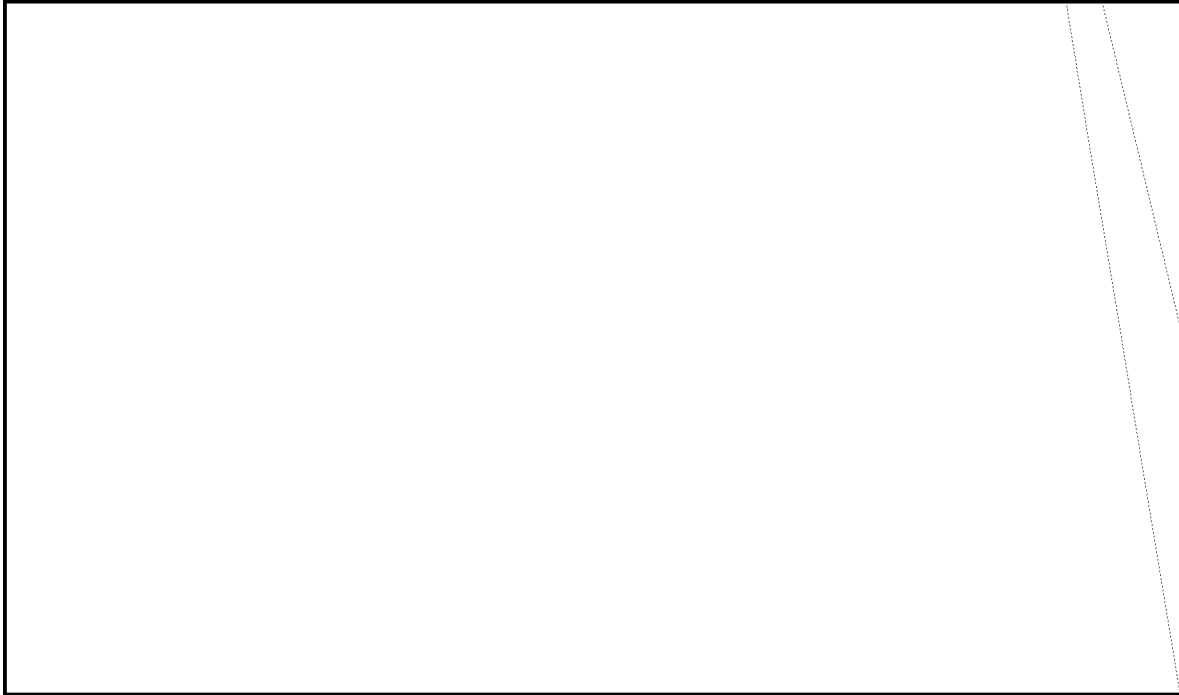
20. Between August and November of 1951 there were several exchanges between USCIB and LSIB in the course of obtaining [] approval for this approach to the []. The final USCIB Ad Hoc Committee Report was forwarded to LSIB on 17 August, and the details of the proposed plan developed by State and CIA were explained to Sir Edward Travis, and forwarded by him to [] on 1 November. Meanwhile LSIB had considered the USCIB proposal and had advised USCIB, by a message of 5 November (23/28), that this plan was not acceptable to them. They felt that the approach was too risky and would not serve to accomplish the over-all improvement in the security of [] communications which they considered imperative. At the urging of Sir Edward Travis LSIB reconsidered the detailed plan and, by a message of 8 November and a subsequent letter of 19 November (23/40), withdrew their objections on the understanding that (a) the approach would be addressed solely to correcting [] abuse of NATO communications security practices

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

~~TOP SECRET SECURITY INFORMATION CANCE~~

16.

and (b) would be followed by further consideration of the British suggestion that steps should be taken to improve over-all communications security. By letter of 23 November (23/41) USCIB advised LSIB that the approach would be made shortly after 1 December.

~~TOP SECRET SECURITY INFORMATION CANCE~~

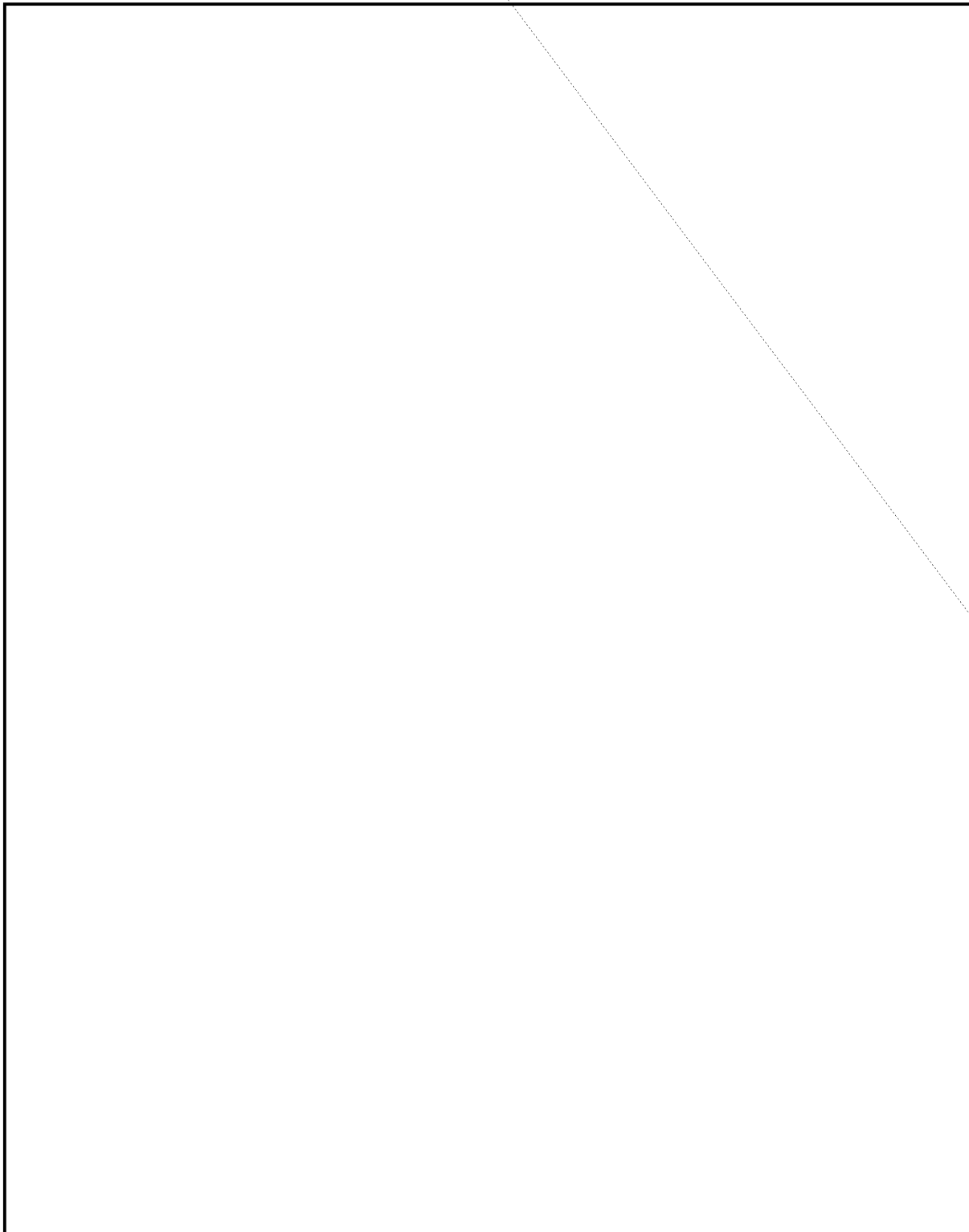
~~TOP SECRET SECURITY INFORMATION CANOE~~

17.

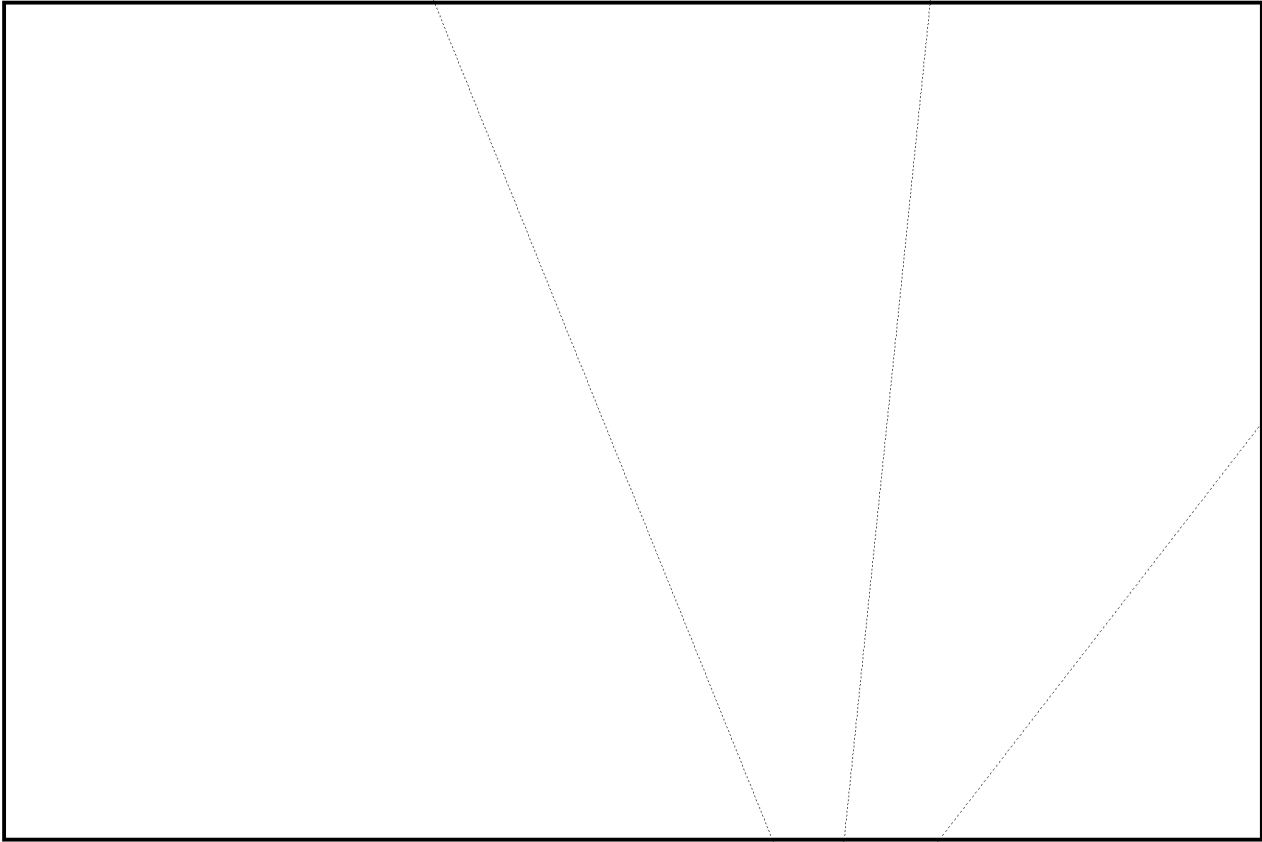
of [redacted] response and recommending that it would be best to consider the matter closed until further instances of [redacted] abuse of NATO communications security procedures appeared.

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

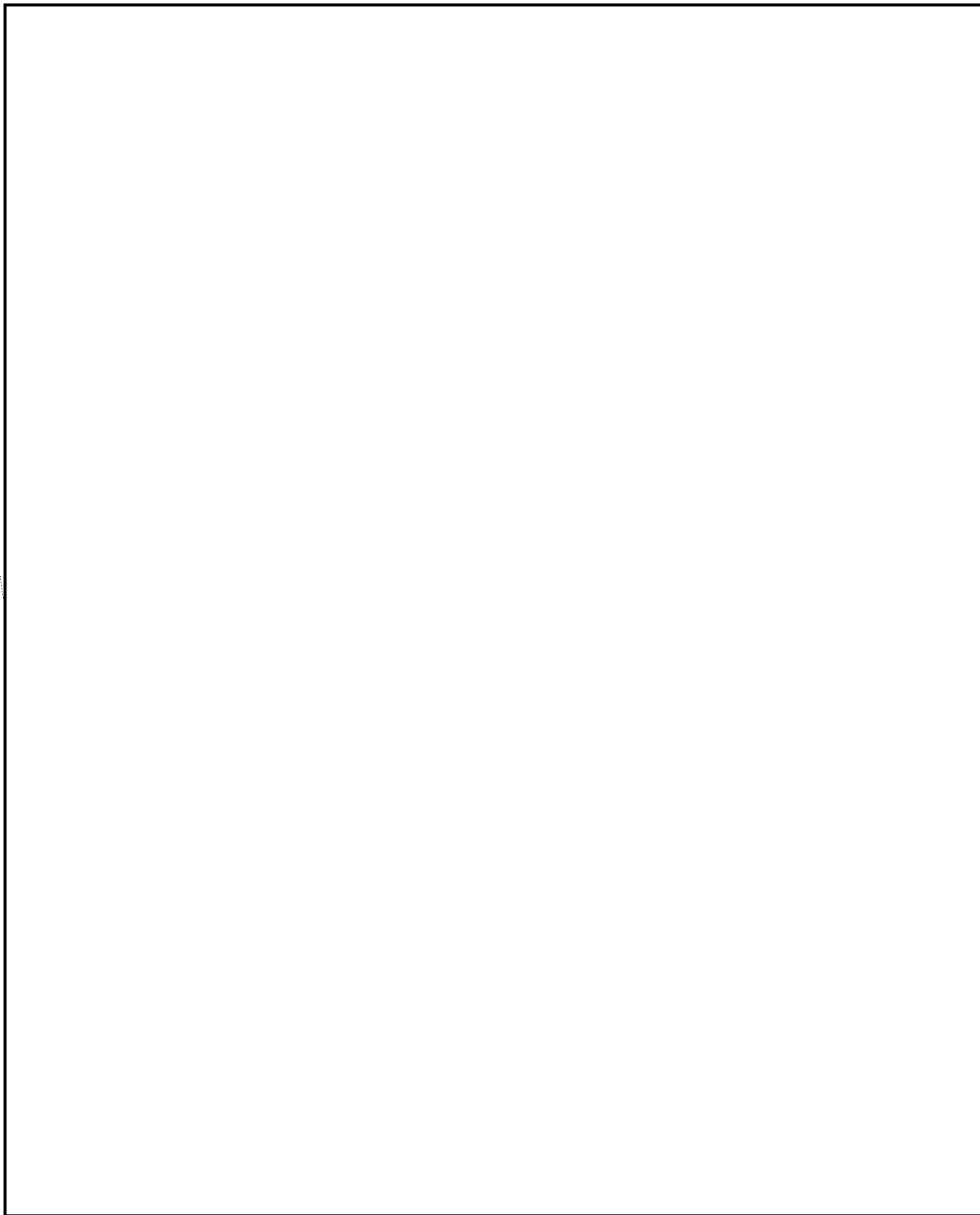
~~TOP SECRET SECURITY INFORMATION CANOE~~



through the provision of the combined cipher machine (CCM), but stated that there were only 10 CCM's which could be made available at that time and that it was not possible to anticipate when further equipment would be available to satisfy the entire [redacted] request. The DIRAFSA stipulated that this equipment could be made available only on a free loan or rental basis and that the [redacted] Government would have to agree to certain stipulations covering the physical protection and disposition of it.

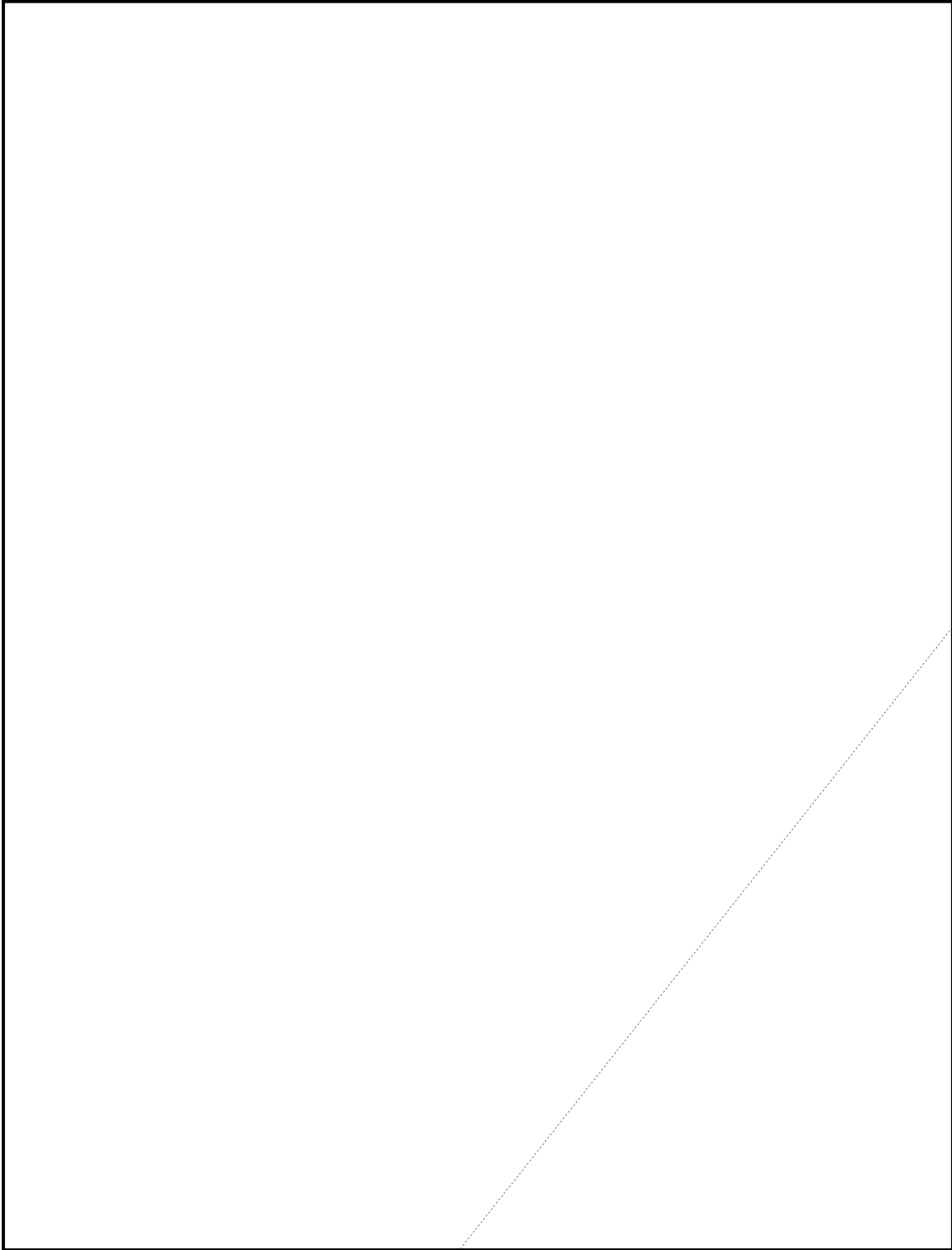
~~TOP SECRET SECURITY INFORMATION CANOE~~EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET SECURITY INFORMATION~~



~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~



~~TOP SECRET SECURITY INFORMATION CANOE~~

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

that, in reaching a decision in this case, it had been impelled by the "prolonged US-UK discussions on this general problem in the past" to feel that "the importance to the US and UK of the security of the communications of

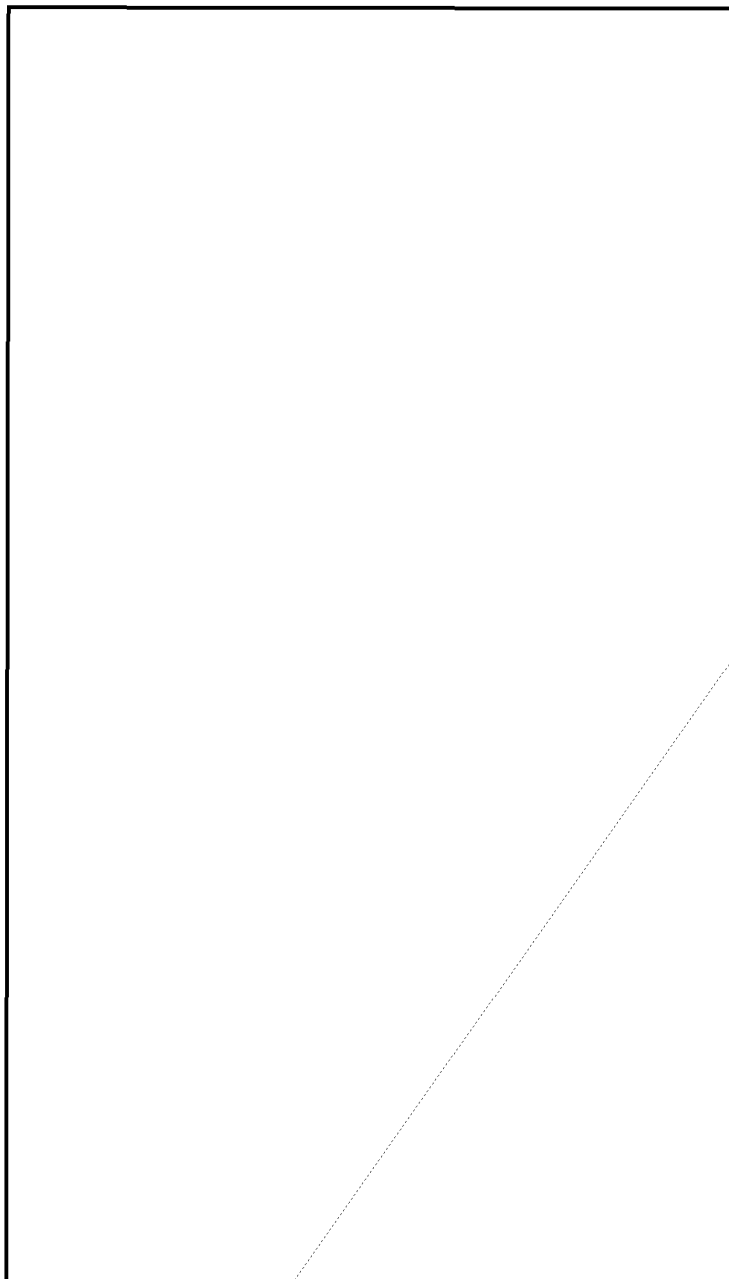


EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET SECURITY INFORMATION CANOE~~

EXHIBIT 1

SECURITY VIOLATIONS



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

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~EXHIBIT 2EO 3.3(h)(2)
PL 86-36/50 USC 3605STATUS OF NATO CRYPTOSYSTEMS

A. First level (high military and diplomatic):

1. Typex with Simplex settings.
2. Some one-time pads (approved by standing group).

Date of approval: 20 July 1950.

[REDACTED]

NOTE: Non-BRUSA countries were furnished full technical details for making up their own national Simplex settings but no information is available as to whether they are doing so.

B. Second level (military only -- high command to divisions):

1. CCM.

Date of approval: 10 November 1951.

[REDACTED]

2. Natex (back up to CCM).

Date of approval: 25 July 1952.

[REDACTED] September 1952.

C. Third level (low echelon):

1. Natex.

Date of approval: 25 July 1952.

No systems yet provided.

2. French modified M-209.

Date of approval: Early 1952

Effective only by [REDACTED] so far.

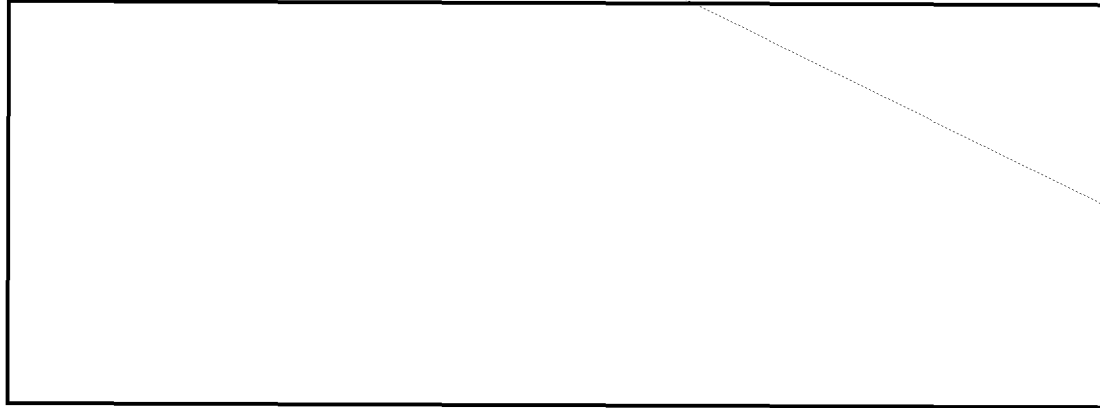
~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

D.

E.

F.



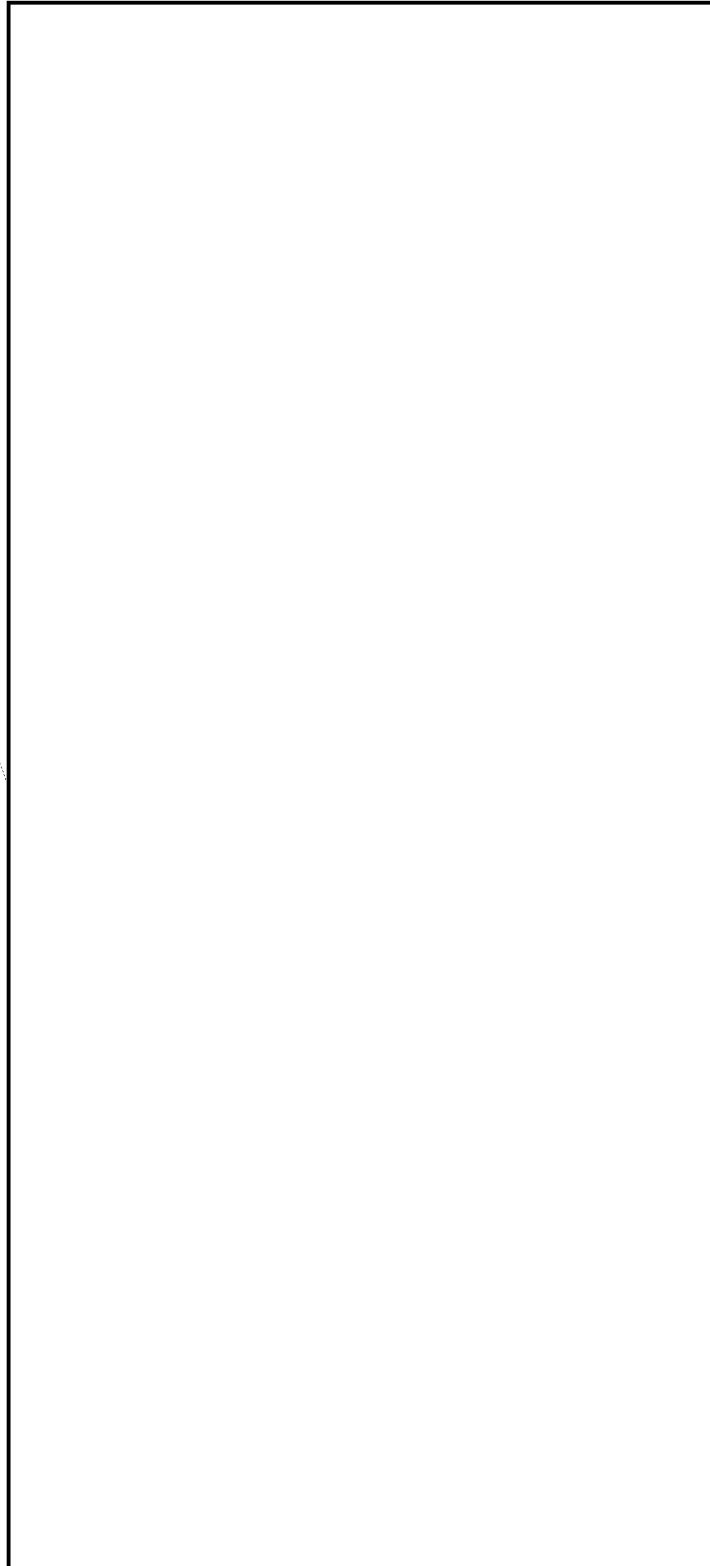
~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANCE~~

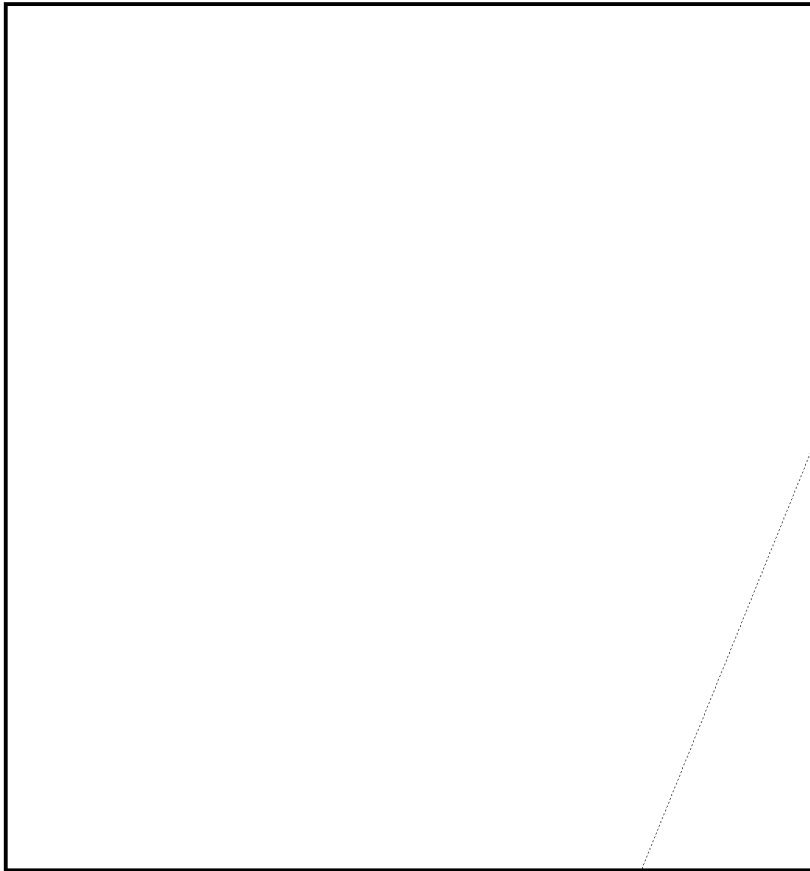
EO 3.3(h)(2)
PL 86-36/50 USC 3605

EXHIBIT 3

MESSAGES CONTAINING DAMAGING INFORMATION



~~TOP SECRET SECURITY INFORMATION CANOE~~



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

~~TOP SECRET SECURITY INFORMATION CANOE~~