

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

AFSA-OOT/ef

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

2 July 1951

MEMORANDUM FOR: Chief, AFSA-02

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

SUBJECT: Hagelin machines, study of

Reference: T/S AFSA memo to Director, CIA, serial 000154, dated 25 June 1951, subj: Negotiations with Mr. Hagelin

1. In view of paragraph 2 of the reference, it is desired that you review AFSA's position with respect to its cryptanalytic potential in handling traffic enciphered on crypto-machines manufactured and sold by A. B. Cryptoteknik (the Hagelin Cryptograph Company) of Stockholm and submit on or before 1 September 1951:

a. An operations plan for intensifying AFSA's present efforts to solve the traffic enciphered by the current Hagelin machines;



2. The plans should be carefully integrated and should indicate:

a. The estimated approximate number of additional personnel that may be required and how they would be employed;

b. The additional or new cryptanalytic machines or aids that may be required to assist in solution.

c. The estimated approximate amount of additional space and funds required for a. and b.

3. It is desired that AFSA-03, AFSA-OOT and the Chief, AFSA-14 assist in this project by participating in conferences pertaining thereto and in the preparation of the final plans. A preliminary report is desired not later than 31 July 1951.

Earl E. Stone

EARL E. STONE

Rear Admiral, U.S. Navy

Director, Armed Forces Security Agency

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

Copy to:

- AFSA-00A AFSA-03
- AFSA-00B AFSA-11
- AFSA-00C AFSA-12
- AFSA-00T AFSA-14

~~U. S. EYES ONLY~~

22 May 1951

MEMORANDUM FOR: See Distribution List

SUBJECT: Negotiations with Mr. Hagelin

ENCLOSURE: Draft Report by William F. Friedman, Technical Consultant, to DIRAFSA on the Aktiebolaget Cryptoteknik, Stockholm, Sweden (The Hagelin Cryptograph Company)

1. A meeting has been called by DIRAFSA for the purpose of discussing the enclosure and assisting DIRAFSA in establishing the position he should take at this time in regard to the subject negotiations.

2. The meeting will be held in the AFSA Conference Room (19-125), on 23 May 1951 at 1400 hours.

3. DIRAFSA desires that you review the enclosure in advance of the meeting so as to be prepared to participate in the discussion.

4. The enclosure should NOT be circulated within your office or division.

William F. Friedman
 WILLIAM F. FRIEDMAN
 AFSA-OOT

AFSA-00A
 AFSA-00B
 AFSA-00C
 AFSA-02 (Capt. Holtwick)
 AFSA-021 (Mr. Rowlett)
 AFSA-03 (Capt. Harper)
 AFSA-04A (Dr. Sinkov)
 AFSA-41 (Mr. Austin)
 AFSA-11 (Capt. Goodwin)
 AFSA-14 (Capt. Dyer)
 Copy for: DIRAFSA

Copy 4 

~~U. S. EYES ONLY~~

~~TOP SECRET~~

~~U. S. EYES ONLY~~

APPENDED DOCUMENT CONTAINS
CODE WORD MATERIAL

~~U. S. EYES ONLY~~

~~TOP SECRET~~

REPORT BY WILLIAM F. FRIEDMAN, TECHNICAL CONSULTANT, TO THE DIRECTOR,
ARMED FORCES SECURITY AGENCY ON THE AKTIEBOLAGET CRYPTOTEKNIK, STOCKHOLM,
SWEDEN (The Hagelin Cryptograph Company) dated 22 May 1951

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

INDEX TO CONTENTS

	<u>Paragraphs</u>	<u>Pages</u>
REPORT TO THE DIRAFSA	1-4	1-3
THE PROBLEM	1	1
FACTS BEARING ON THE PROBLEM AND DISCUSSION	2	1
CONCLUSIONS	3	1-3
RECOMMENDATIONS	4	3
ENCLOSURE "A" (TO BE PROMULGATED)		44
ENCLOSURE "B"		5-20
INTRODUCTORY REMARKS	1-2	5-6
THE COMINT POSSIBILITIES	3-8	6-12
<div style="border: 1px solid black; width: 400px; height: 100px; margin: 5px 0;"></div>	4-5	6-10
	6	10-11
	7-8	11-12
THE COMSEC POSSIBILITIES	9	12-13
<div style="border: 1px solid black; width: 400px; height: 20px; margin: 5px 0;"></div>	10	14-15
ASSESSMENT OF ADVANTAGES, DISADVANTAGES, AND RISKS	11-18	15-19
FINAL REMARKS	19-22	19-20
Annex 1		21-23
ENCLOSURE "C"	1-10	24-28
Annexes 1-5 (not included in document)		
ENCLOSURE "D"		29-34

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

REPORT

BY

WILLIAM F. FRIEDMAN

TECHNICAL CONSULTANT

TO THE

DIRECTOR, ARMED FORCES SECURITY AGENCY

ON THE

AKTIEBOLAGET CRYPTOTEKNIK, STOCKHOLM, SWEDEN
(The Hagelin Cryptograph Company)

- References:
- (a) USCIB 13/157
 - (b) AFSAC: 66/15
 - (c) AFSAC: 66/20
 - (d) AFSAC: 66/23

THE PROBLEM

1. a. To determine the advantages, disadvantages, and risks to the

U.S.

[Redacted]

- b. To assess those advantages, disadvantages, and risks;

- c. To determine

[Redacted]

and

- d. To evaluate and render an opinion as to the suitability of a

[Redacted]

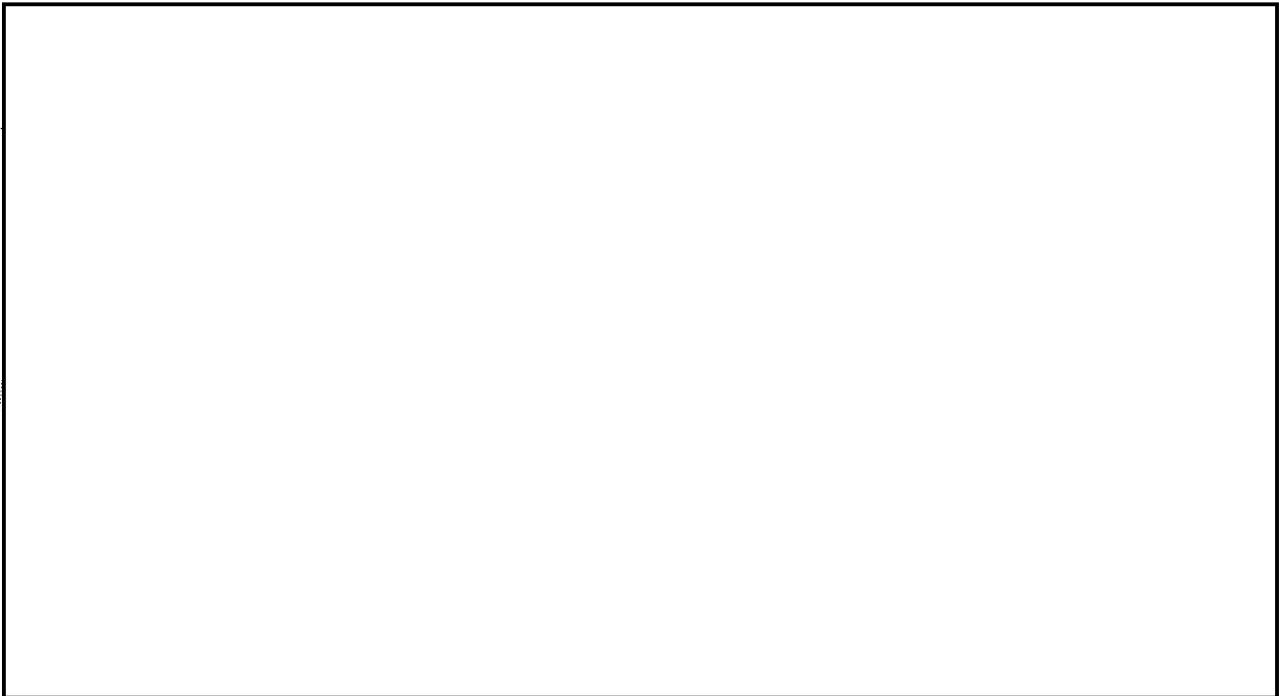
FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B".

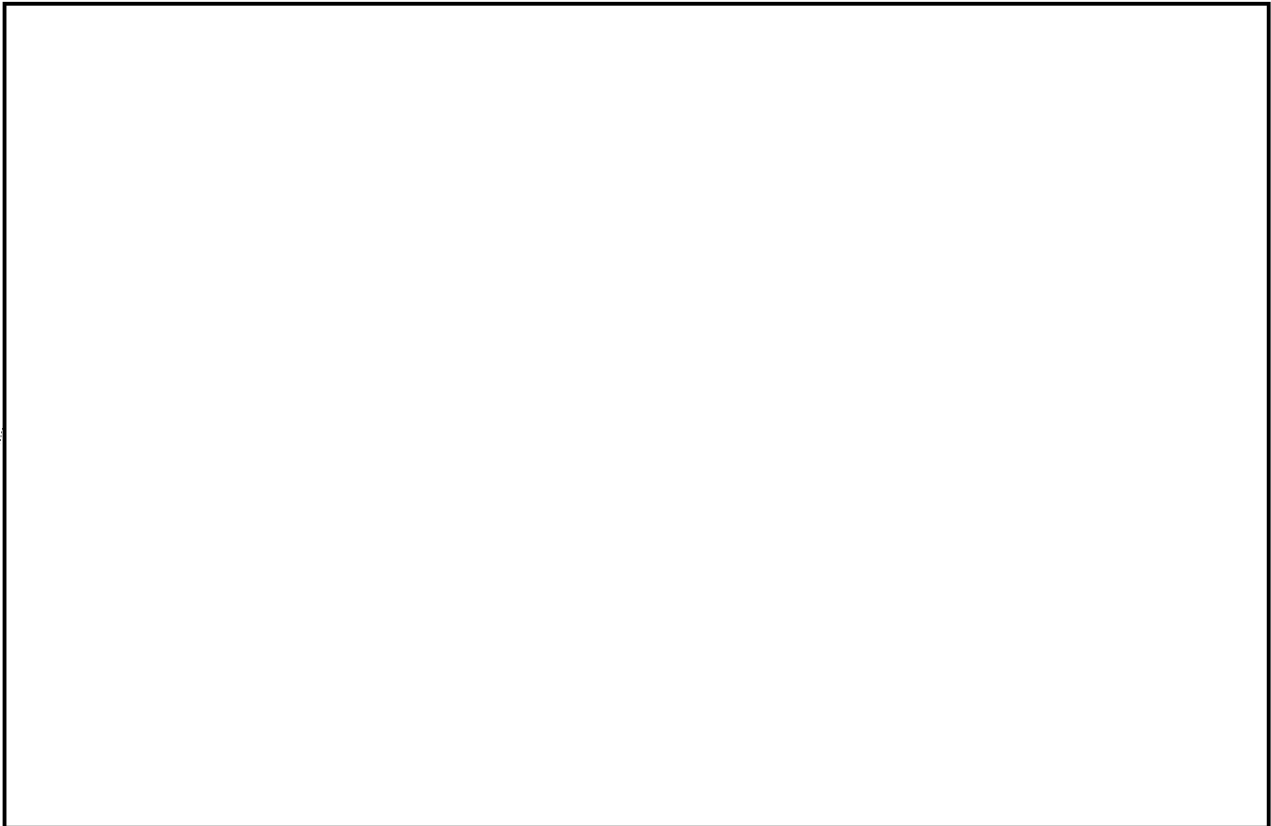
CONCLUSIONS

3. It is concluded that:

- a. It would be to the advantage of the U.S. Government if the proposed new or improved Hagelin cryptoequipments were prevented from being developed, manufactured, and sold commercially on the open market.

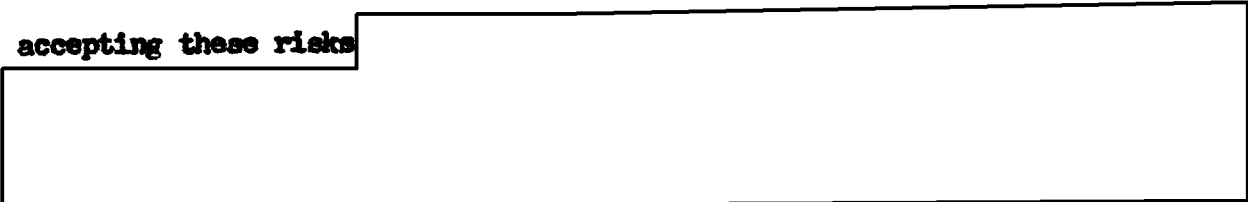


(3) Employing the experience and technical know-how of Hagelin and the HCC in the production of communication security equipment for possible employment in connection with NATO requirements, as well as for the possible use of U.S. military and civil agencies.



e. Assessment of the advantages, disadvantages, and risks warrants

accepting these risks



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

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

g. The cost of the contemplated deal, \$700,000, would not be excessive, in view of its potential benefits to the U.S. Government.

h. The Director, Armed Forces Security Agency (AFSA) should forward this Report to the Director of Central Intelligence and to the other members of USCIB for information.

j. If a deal is consummated, this project should be given a code name and be surrounded with COMINT special security restrictions.

RECOMMENDATIONS

4. It is recommended that:

a. Enclosure "A" be forwarded to the Director of Central Intelligence;

b. This report be forwarded to USCIB for the information of member agencies other than CIA and AFSA;

d. This project be assigned a cover name and be given special COMINT security protection.

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

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

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

~~RESTRICTED~~

◊PROMULGATION OF ENCLOSURE "A" WILL BE EFFECTED BY THE DIRAFSA
FOLLOWING THE MEETING ON WEDNESDAY, 23 MARCH 1951

4

Enclosure to AFSA-00T Staff Study
dtd 22 May 1951

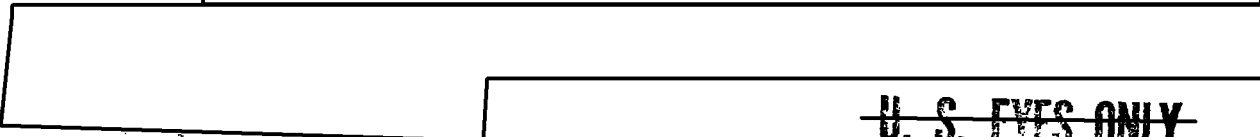
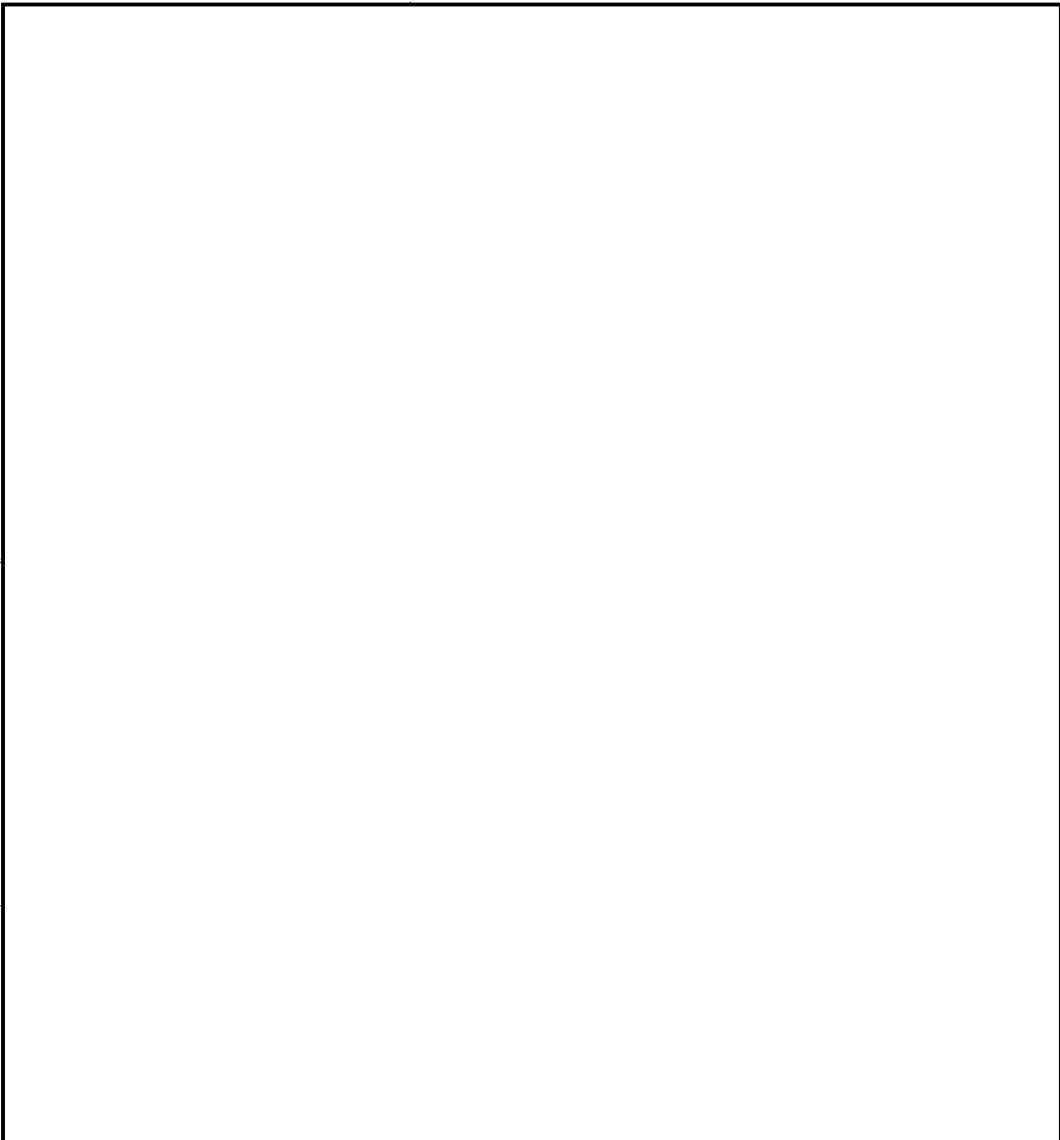
ENCLOSURE "A"

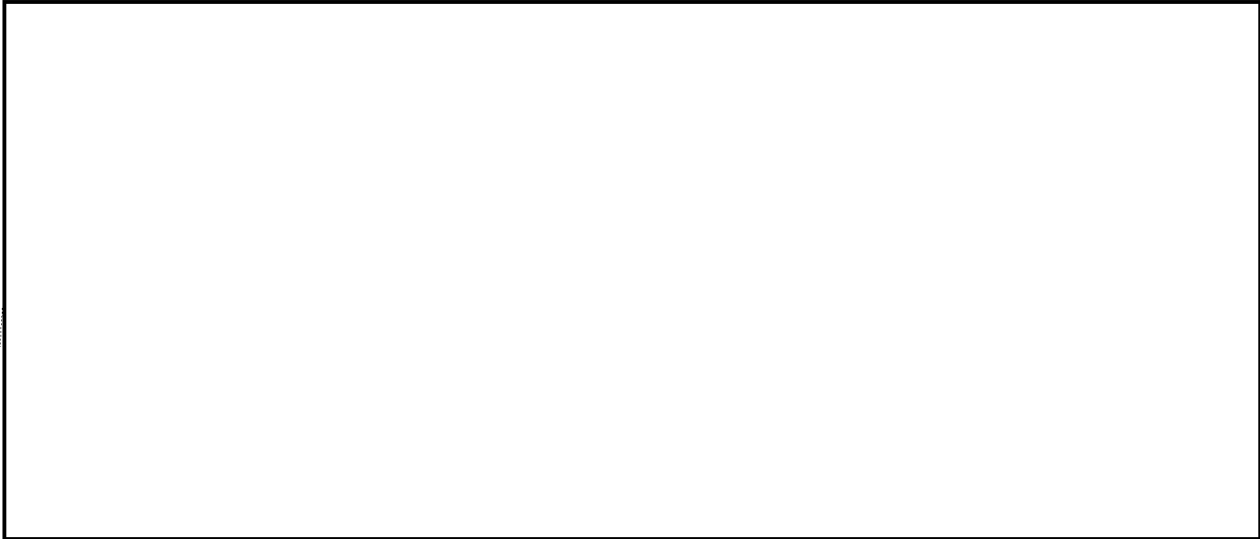
~~RESTRICTED~~

INTRODUCTORY REMARKS

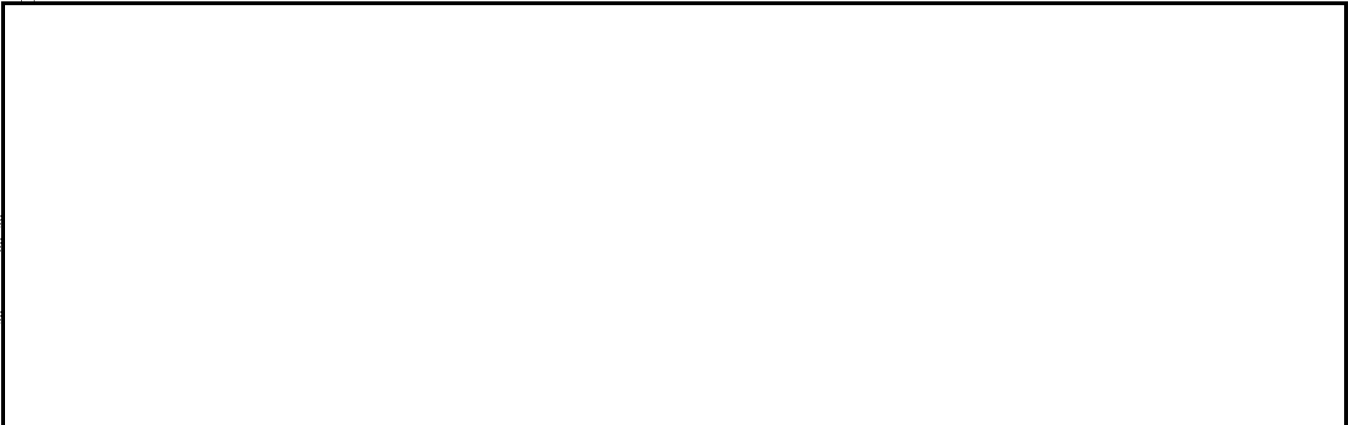
1. At the Sixty-first Meeting of USCIB, held on 9 March 1951, a statement regarding certain negotiations with Mr. Boris C.W. Hagelin, hereinafter referred to as Hagelin, who is sole owner of the Hagelin Cryptograph Company (HCC), was presented by a representative of the Armed Forces Security Agency (AFSA), on behalf of the USCIB Coordinator. A brief history of the negotiations with Hagelin forms Enclosure "C" to this report; in Reference (a) will be found the minutes dealing with this item of the agenda of the meeting.

2. a. These negotiations have now resulted in a draft memorandum of agreement, a copy of which forms Enclosure "D" of this report. Briefly, under this draft, for the payment of \$700,000 plus a "best efforts" undertaking with respect to the surplus commercial sale of M-209 machines, the U.S. would



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

b. Each of these categories of potential benefits will now be studied in detail.



b. The HCC is now the only firm in the world which develops, manufactures, and commercially sells cryptographic equipment. The firm is well-established and has attained a position of importance in the COMSEC equipment field. Since the end of hostilities in World War II, Hagelin has made a number of inventions and is contemplating developing, manufacturing, and selling improved models of present Hagelin machines and certain new types of machines. These will be briefly described in the next paragraph, and discussed only insofar as concerns their bearing on the problem under consideration.

5. a. The HCC is preparing to manufacture and sell an improved model of the present C-38 machine, in which not only the new keying mechanism but

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

also several additional complicating features would be incorporated.



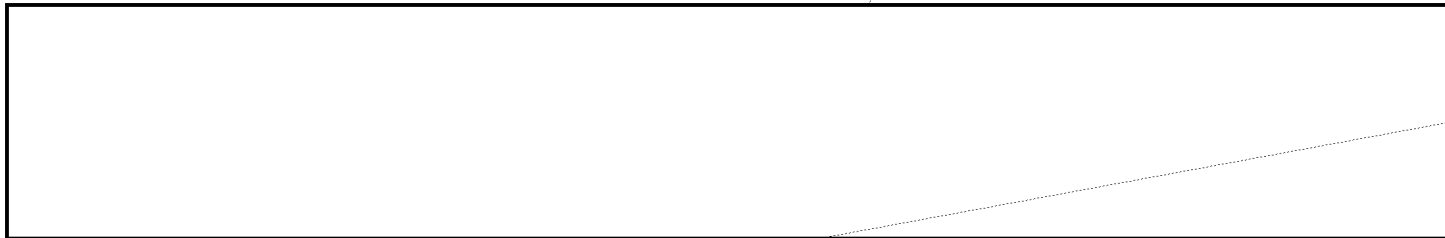
The effect of this on U.S. sources of COMINT would probably be important, as discussed below:



b. The HCC proposes to employ the new keying mechanism as a basis for the control of the cryptographic elements of not only the new model C-38 but also of several new types of cipher machines. In particular, the



using the new keying mechanism. The possible effects are discussed below:



~~U.S. EYES ONLY~~

[Redacted]

It is possible that two or three years will be required for development and that several years will elapse before this machine would be available for sale.

(2) With regard to

[Redacted]

At present the HCC has a development model in which the new keying mechanism has been incorporated. However,

[Redacted]

It is not possible, without more detailed information, to evaluate the security of this new machine.

c. The HCC has developed a model of the C-38 which uses a perforated tape for keying control instead of the present "pin and lug" keying mechanism. "One-time" use of the tape will produce a "one-time system" and, provided the tapes are properly made, messages enciphered on such a machine will be unsolvable. A key-tape generator has also been developed for producing the tapes to be used with this machine.

[Redacted]

d. The HCC has also developed a machine for producing "one-time pads" of the numerical type

[Redacted]

for "literal pads". The principles underlying the model already produced are good but further study and more details are necessary before a firm security evaluation can be made.

[Redacted]

provided the machines are so constructed as to assure non-predictability of keying sequence.

e. It is true that the U.S. and the U.K. Governments are now taking steps to improve the COMSEC of the other members of NATO and the result of

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

~~U.S. EYES ONLY~~

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

effective measures toward that end

[Redacted]

[Redacted]

[Redacted]

f. The effects of an expanding market for Hagelin machines should not be overlooked, especially as regards the possibility that they will be purchased by certain of the satellites of the U.S.S.R. It is understood that Poland, for example, is now a potential HCC customer. It would certainly

[Redacted]

available to such countries,

[Redacted]

g. What has been said in the preceding subparagraph applies particularly if the proposed new types of Hagelin machines were adopted and used by U.S.S.R. satellites, or by non-NATO governments currently friendly to the U.S. Traffic in the new rotor machine, for example, would probably be entirely unreadable.

h. Finally, if the HCC should put on the market a good one-time tape machine and good equipment for making the tapes, or a good one-time pad producing machine, their widespread use would, in a few years, probably make

[Redacted]

[Redacted]

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

~~U. S. EYES ONLY~~

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

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

~~TOP SECRET ACORN~~

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

continuation of present sources.

Gathering of cryptologic technical intelligence

6. a. During the past 25 years Hagelin, in exploiting the products of the HCC, has established contact with the cryptologic authorities and agencies of many governments. It appears that some of the agencies with which Hagelin has dealings are not so security-minded as we are, and certain general or specific matters are disclosed to him as information about which there is no secrecy. He has thus been able to gather not only general ideas with respect to the size and activities of the organizations, their attachment, etc., but also specific information as to chief personalities, equipment, practices, requirements, etc.

c. The HCC has agencies in several countries in each hemisphere.

These also serve as information-gathering elements.

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

~~U. S. EYES ONLY~~~~TOP SECRET ACORN~~ ¹⁰ ENCLOSURE "B"

[Redacted]

e. It may be possible to gain technical intelligence applicable to the cryptologic agencies of U.S.S.R. satellite countries. In this connection,

[Redacted] representatives of the U.S.S.R. have visited the HCC since 1946, desiring information as to new HCC developments and products.

f. It should also be added that the HCC frequently receives requests for specific developments. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

7. a. The use of cipher machines for COMSEC purposes is steadily increasing with greater mechanization of office work in general. If the governments

[Redacted]

b. In this connection, it should be noted that not only does the HCC solicit business, but also some business comes without solicitation from governments desiring specific developments or improvements. This situation

[Redacted]

~~U. S. EYES ONLY~~

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

8. The potential COMINT benefits mentioned above are those which are more or less obvious. It is impossible to anticipate or prognosticate all the COMINT benefits [redacted]

[redacted] The disadvantages and/or risks inherent in such an arrangement will be treated in paragraphs 10-15 below.

THE COMSEC POSSIBILITIES

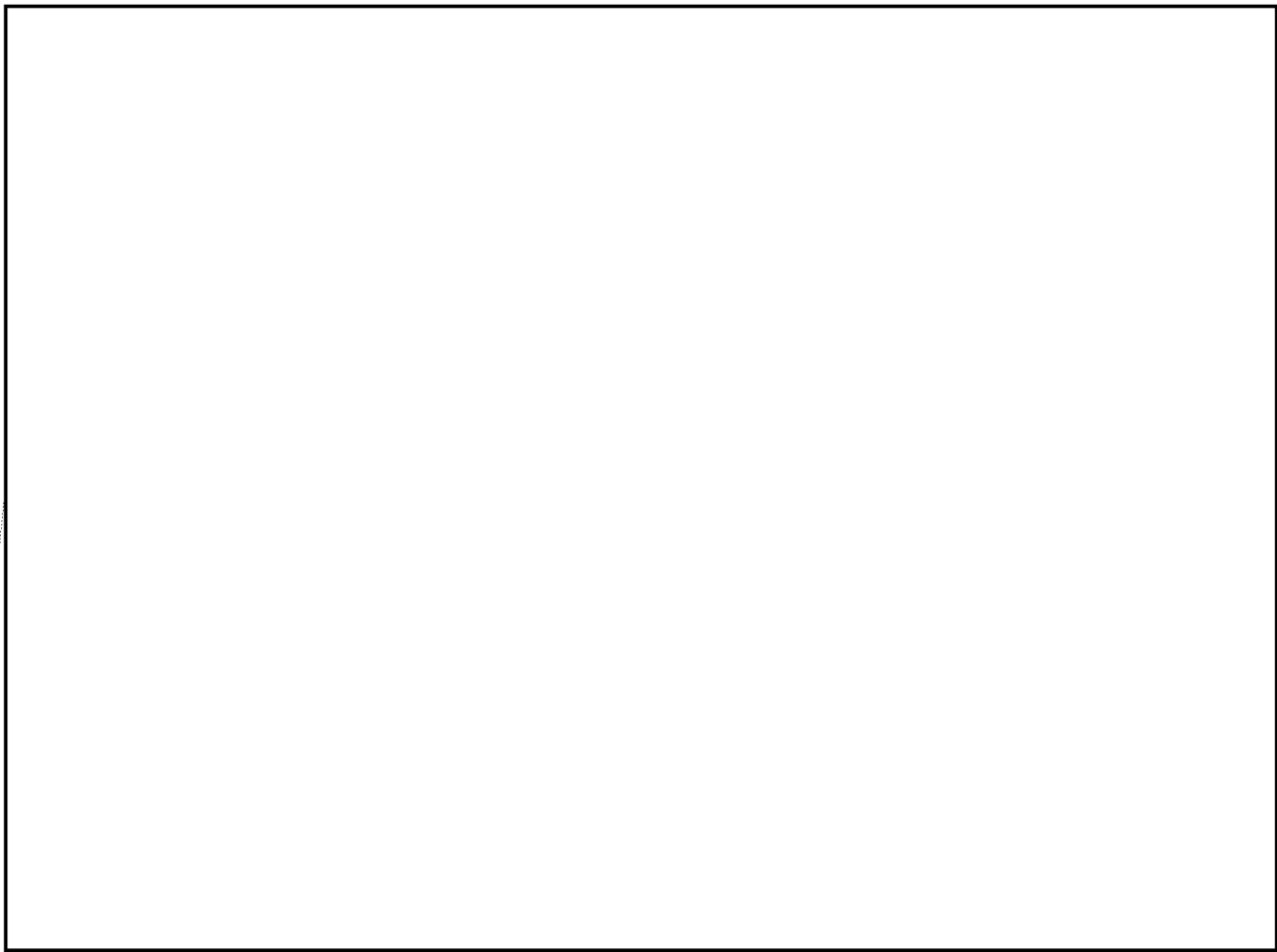
9. a. Hagelin has proved himself a clever engineer and designer, as well as a cryptographer with some appreciation of the technical intricacies and pitfalls in the COMSEC field. [redacted]

b. Reference has been made to the new keying mechanism and other improved features for the modified M-209 (or C-38) machine. Although AFSA is still studying the prototype improved C-38 machine submitted by Hagelin early in 1951, it is already permissible to state that it represents considerable improvement over the present C-38 (or M-209). AFSA's present COMSEC interest in this improved model lies in the possibility of incorporating the new keying mechanism and certain other recently proposed additional new features in an AFSA development called the Mechanical Cipher Machine (MCM), which is being designed specifically for the U.S. Marine Corps and for limited use by the U.S. Navy. It is quite probable that the original U.S. contracts with Hagelin (those of 1941/42) permit the U.S. to use his recent improvements on the M-209 without additional recompense to him; it is also true that Hagelin has indicated he would not contest this point. However, it must be noted that the U.S. contemplates using those improved features not in the M-209 but in the MCM -- a quite different machine. Whether this changes the patent situation is not clear. In any case, however, Hagelin's consultative assistance in working out the incorporation of these improvements in the MCM, and in other special cases, would probably be quite useful.

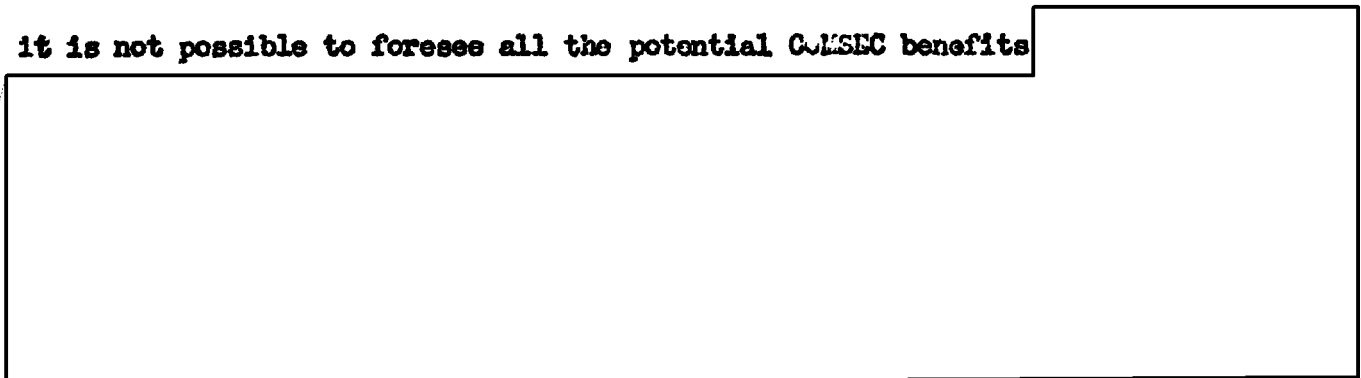
c. When the AFSA development known as AFSAM-7 has been completed and the machines have been procured and distributed to holders, our large stock of M-209s will become available for other purposes or usages. If the surplus M-209s were converted to modified M-209s, principally perhaps by

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

incorporating the new Hagelin keying mechanism, they might be given to NATO countries for use in low-level NATO or low-level national communications. Possibly the M-209 might be used in encrypting NATO weather traffic. We probably have a sufficient stock to supply all NATO armed forces with these machines. The HCC might be useful in working out the incorporation of the improvements, although it has been stated by Hagelin that, from an engineering point of view, it would be more practicable to build machines anew rather than attempt to modify the present ones. Perhaps additional work along these lines will demonstrate the feasibility of incorporating the improvements, or certain of them, in our present M-209s.



f. As indicated in connection with the potential COMINT benefits, it is not possible to foresee all the potential COMSEC benefits



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

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

[REDACTED]

from the nature of certain risks that must be faced. The risks are three-fold:

(1) Possible waste of money.- The deal would cost \$700,000 and

[REDACTED] and (b) unforeseen contingencies might arise to prevent, obstruct, or reduce its efficacy, there would be the risk that the money would have been spent in vain. This risk is discussed in detail in paragraphs 11-14 below.

(2) [REDACTED]

[REDACTED] This risk is discussed in detail in paragraph 15 below.

[REDACTED]

in detail in paragraph 16 below.

b. There is another apparently significant but in reality unimportant disadvantage [REDACTED] the placing of a limitation on U.S. disposition of surplus M-209 machines. [REDACTED]

[REDACTED] "undertakes to use its best efforts to prevent the surplus sale or other disposition for private or commercial use and/or resale of any M-209 machines now owned by the United States or any Agency thereof." This condition, while appearing to be a limitation on U.S. rights, is really in furtherance of U.S. interests. [REDACTED]

[REDACTED] it is existing policy not to permit these machines to be sold as surplus equipment. Annex 1 to this Enclosure has a bearing on this point.

c. One other disadvantage may be mentioned, viz., the additional administrative burdens which must be assumed by the U.S. if full advantage is to be taken [REDACTED]

~~TOP SECRET ACORN~~

~~U. S. EYES ONLY~~
ENCLOSURE "B"

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

study reports, etc. This would involve additional personnel, not many, but perhaps two or three persons.

ASSESSMENT OF ADVANTAGES, DISADVANTAGES, AND RISKS

11. a. With reference to the risk mentioned in paragraph 10.a(1), it is clear that as regards the potential benefits which might flow from the [redacted] if there was certainty as to their realization, a [redacted] would be well worth undertaking, even at considerable cost. However, it is obvious that not only can there be no such certainty, but also that the probability of reaping the potential benefits is undeterminable, since much would depend upon:

OGA

[redacted]

12. a. With regard to the factor of integrity, it can be stated with some assurance that in previous dealings with Hagelin he has demonstrated his trustworthiness and good faith. All who have talked with him agree that, although a good trader, he can be relied upon to execute, in good faith and to the fullest extent of his ability, the terms of any agreement to which he is a willing party. As regards the integrity of Hagelin Junior, there is not only no reason to entertain doubts on this score but also the parental control exercised over him is such that for the term of the agreement at least there should be no difficulties.

b. With regard to other personnel of the HCC, we have the assurance of the Hagelins that none of them, save, possibly, Mr. C.E. Lindmark, is capable of inventing or developing new ideas in the COMSEC equipment field.

[redacted]

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~~~EYES ONLY~~

[REDACTED]

13. With regard to the bearing that the action which the U.S. Government is taking with respect to NATO communications [REDACTED]

[REDACTED] the following comment may be pertinent: Hagelin has developed and is developing certain cryptographic equipment which, [REDACTED]

[REDACTED]

In the case of the pro-Soviet nations, the possible effects, whether for better or worse, of Hagelin's developments are, of course, completely unpredictable.

[REDACTED]

considered: suppose that some well-equipped firm should decide to go into the COMSEC equipment business and become a competitor of the HCC. Then, either,

[REDACTED]

as having been a poor investment. The latter would, no doubt, be the decision.

b. The chances for the occurrence of this contingency, however, are small in view of the head-start the HCC now has and the comparatively very limited market for COMSEC equipment. Moreover, even should it occur, the probability that the new firm will have developed, tested, manufactured, and be ready to sell its new product in quantity within a very few years is rather

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

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

small, if our experience in such matters is taken into account.

c. Other contingencies which would nullify or minimize the benefits

[redacted] For example, the Swedish Government, or conceivably the U.S.S.R., might take over the HCC. Suppose the former occurs: in this event, it is highly probable that the Swedish Government would take action [redacted]

[redacted] Suppose the U.S.S.R. should, as a result of war, take over the HCC. The cryptanalytic situation of the U.S. vis à vis the U.S.S.R. and its various satellites leads to the assumption that we might be no worse off than we are; and it is conceivable that we might be better off.

d. The foregoing four paragraphs discuss the risk mentioned in paragraphs 10.a.(1). There remain to be discussed the risks mentioned in paragraphs 10.a.(2) and (3), and these will be assessed in the next two paragraphs.

15. With regard to the possible damage to U.S. COMINT security in going

[redacted]

The U.S. has control over this in

larger measure.

16. With regard to the risk of political repercussions, it is true that

[redacted]

to certain governments now friendly with this Government, there might be undesirable repercussions. But here again, the danger [redacted] is not believed to be serious, in view of the remarks made in paragraph 12; and if [redacted] the damage to our friendly relations would probably not be severe. As to the risk of undesirable political repercussions that might result [redacted]

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

[redacted] the gravity of
 this risk lies entirely within the control of the U.S., since it will be
 directly proportional to the extent and nature [redacted]
 undertaken. This risk is not an unavoidable concomitant [redacted]
 it can be minimal, or entirely absent, if the U.S. choose not to try to take
 advantage of all the opportunities [redacted]

17. The preceding six paragraphs pave the way for making a judgment

[redacted]

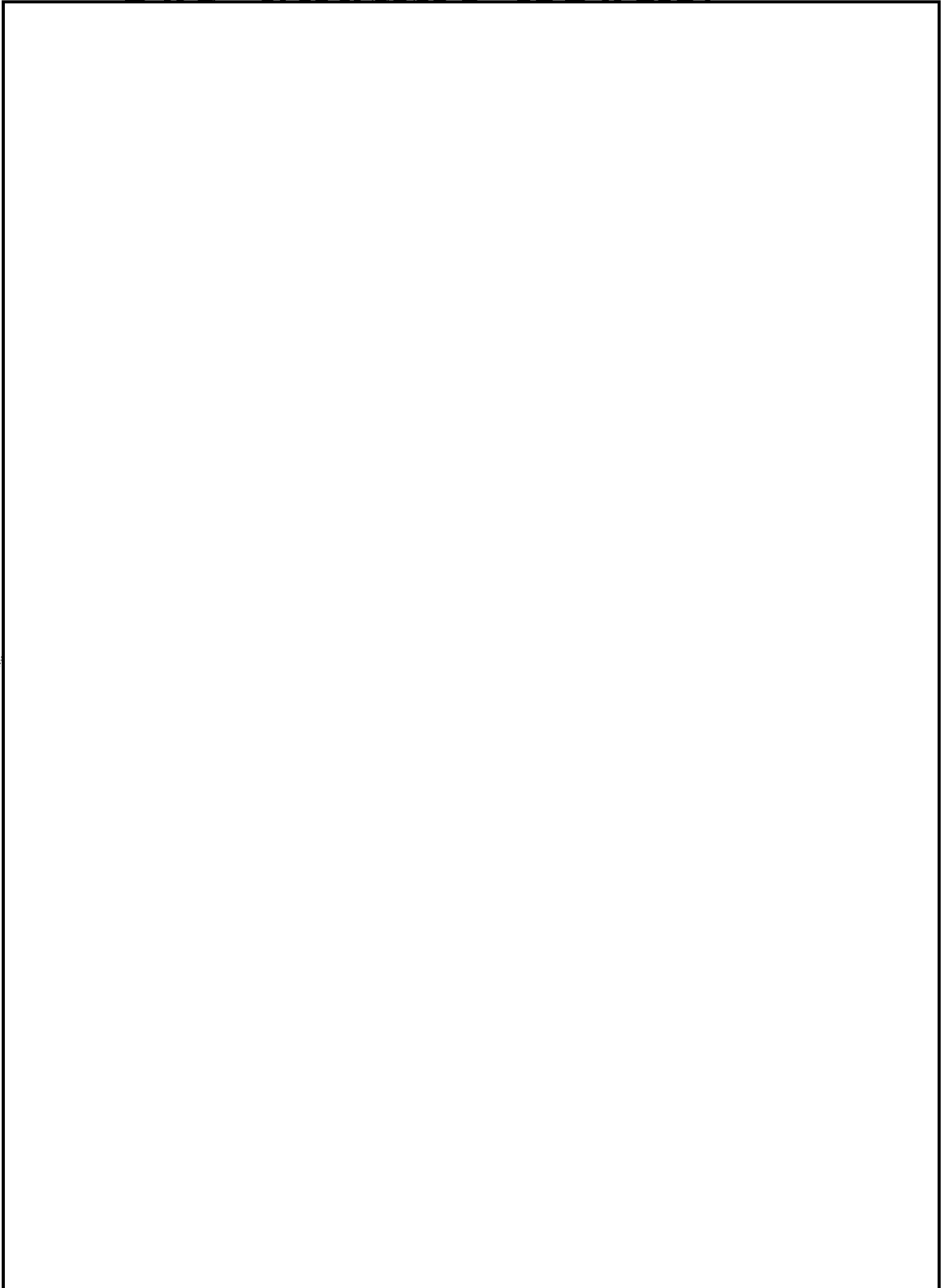
will not have been spent in vain. However, it is my considered opinion that,
 taking into account (a) [redacted]

[redacted] that it

is not inadvisable to assume the risks, and [redacted]
 in expectation that the hoped-for benefits will be realized.

18. a. Enclosure "D", [redacted] was prepared
 by CIA in collaboration with Mr. Hedden on 17 May 1951. It represents an
 improvement on the first draft and, with one exception, it includes all the
 safeguards and features recommended by the Director, AFSA in his memorandum of
 6 April 1951 to the Director of Central Intelligence (Annex 5 to Enclosure
 "C"). This exception is in regard to the terms of payment: the Director,
 AFSA recommended that the consideration be paid in seven equal annual
 installments; CIA finds this not only unnecessary but also undesirable
 from its point of view. Since faithful performance rests in this case on

~~U. S. EYES ONLY~~~~TOP SECRET ACORN ENCLOSURE "B"~~

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

FINAL REMARKS

19. In view of the content of paragraphs 11 to 18 above, it is believed that the Director, AFSA should advise the Director of Central Intelligence that the [redacted] (Enclosure "D") is satisfactory and that, although he still regards [redacted] as a gamble, he deems it to be worthwhile.

20. In view of the interest which USCIB has in this matter, it is deemed desirable to submit this report to the Board merely as information. It is not deemed necessary for the Director, AFSA to submit it to USCIB for approval or

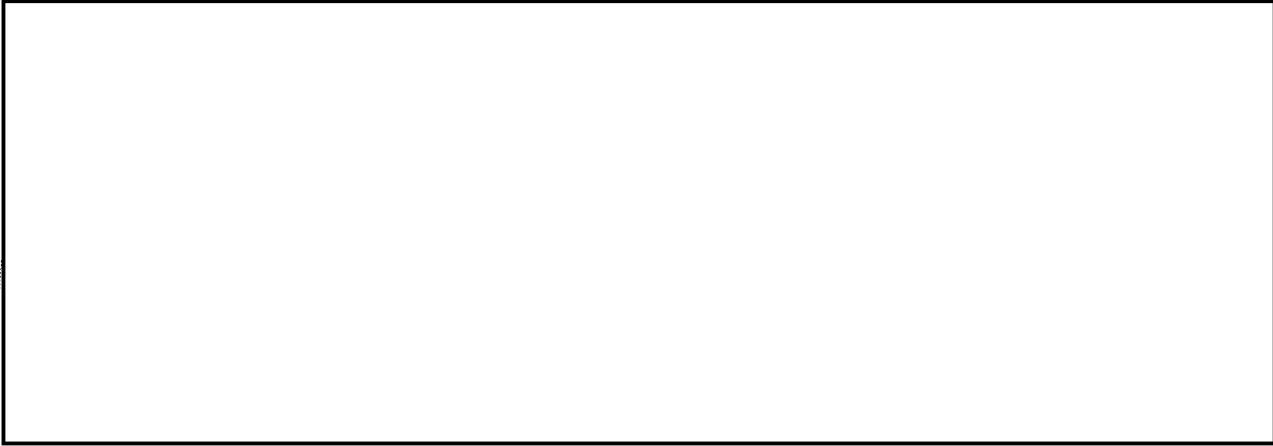
EO 3.3(h)(2)
PL 86-36/50 USC 3605

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

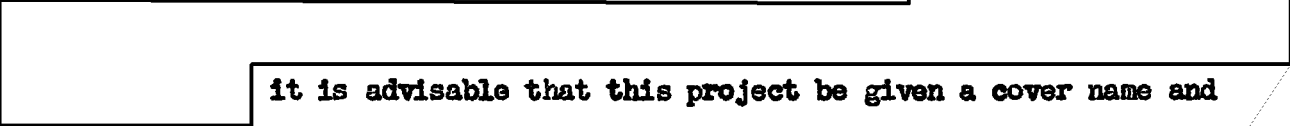
ENCLOSURE "B"


~~U. S. EYES ONLY~~

to attempt to obtain the concurrence or even an expression of endorsement by the Board.



22. In view of the fact that the primary objects



it is advisable that this project be given a cover name and be surrounded with special security safeguards beyond those applicable to COMINT codeword information or material. as few AFSA personnel as practicable should be permitted to know  or any of its details.

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

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

~~U. S. EYES ONLY~~

~~RESTRICTED~~

~~RESTRICTED~~ -- BOOK MSG -25 FEB 46 SENT OUT BY OCSIGO-REQ. DIV. SUPPLY
CONTROL BRANCH

WARK 98567
CM-OUT-98567

CONVERTER M-209 IS CLASSIFIED HEREBY AS MILITARY TYPE I. DESIRE ALL
CLASS A AND B STOCKS BE RETURNED TO U.S. ALL CLASS C STOCKS AND ANY
CLASS A AND B STOCKS NOT RETURNED WILL BE DESTROYED. FOR SECURITY
REASONS NONE SHOULD BE DECLARED SURPLUS TO ANY DISPOSAL AGENCY.

~~RESTRICTED~~

~~TOP SECRET ACORN~~
ENCLOSURE "C"

~~U. S. EYES ONLY~~

BRIEF HISTORY OF

1. a. During World War II, the U.S. Armed Forces extensively employed for low-echelon communications a cipher machine known as Converter M-209. These machines were manufactured by the L.C. Smith and Corona Typewriter Co. at Groton, New York, under U.S. patents owned by Mr. Boris C.W. Hagelin, a citizen of Sweden and sole owner of the Hagelin Cryptograph Company (HCC) of Stockholm.* Approximately 72,000 M-209's were manufactured for the Armed Forces. About 60,000 machines are still on hand, in serviceable condition. The details of the contracts involved in the procurement of the M-209 are given in Annex 1 to this Enclosure.
b. The M-209 is practically identical with a model (C-38) manufactured and sold on the open market by the HCC in various parts of the world, but thus far principally in Europe.
2. a. In its operations in the communications intelligence (COMINT) field, AFSA has knowledge of the extensive use of the C-38 machine by various foreign governments.



3. a. Soon after the close of hostilities, Mr. Hagelin initiated research and development work with a view to improving the C-38 (or M-209) and to producing new types of cipher machines for commercial exploitation.
b. Through informal contact between a member of AFSA and Mr. Hagelin some of Mr. Hagelin's new ideas for cryptologic devices came to the attention of AFSA, and were studied to ascertain their security. The results of such studies were not communicated to Mr. Hagelin.

* The Swedish trade name of the firm is Aktiebolaget Cryptoteknik (A.B. Cryptoteknik).

Enclosure to AFSA-00T
Staff Study dtd 22 May 1951

24

ENCLOSURE "C"

~~U. S. EYES ONLY~~

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~
~~EYES ONLY~~

4. a. On 8 February 1950, representatives of AFSA met with a representative of the Engineering and Technical Service, Office of the Chief Signal Officer, and a representative of Mr. Hagelin, to discuss the possibility of providing Mr. Hagelin with one or more M-209s so that he could incorporate embodiments of certain of his ideas for improving the security of the M-209. The desired machines were not made available but Mr. Hagelin obtained one from the L.C. Smith Company.

b. On 8 January 1951, an M-209, modified by the HCC to incorporate a new keying mechanism, was received by AFSA and promptly subjected to study. Although the security studies have not been completed, it is clear that the new keying mechanism proposed by the HCC would greatly increase the overall security of messages encrypted by the modified machine.

5. a. It was learned that the HCC was preparing not only to manufacture and sell new models incorporating the improved keying mechanism, but also to produce several new cipher machines of considerable security, which also employ the new keying mechanism.

b. It was also learned that patent applications on the new keying mechanism had been filed in several countries (U.S., Switzerland, France, Italy) and



d. In January 1951, Mr. Hagelin, accompanied by his son Boris Hagelin, Junior, came to Washington for the purpose of discussing with AFSA the results of the study of the modified M-209. They were told that the study was not complete and no report was yet available.

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

ENCLOSURE "C"

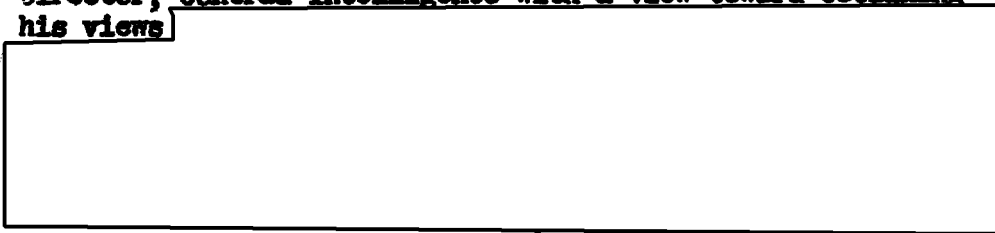


Director, AFSA, who decided to place the matter before the Armed Forces Security Council (AFSAC).

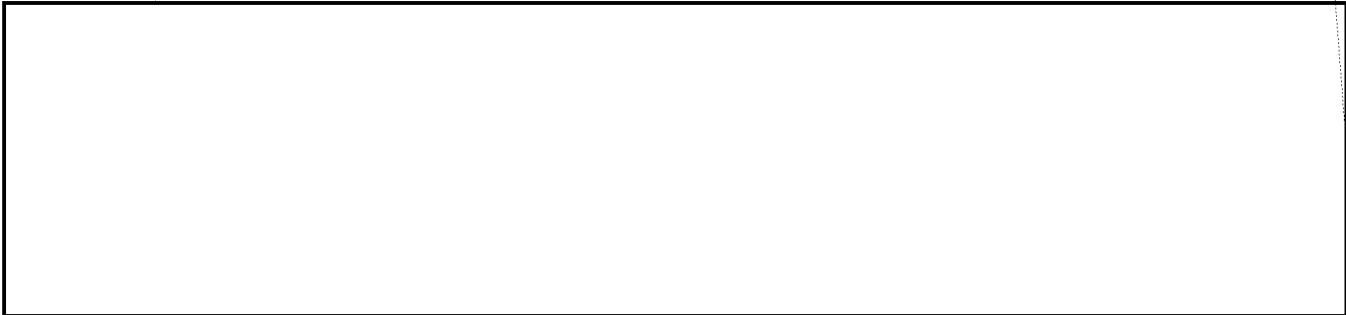
6. a. On 29 January 1951, at the 26th Meeting of AFSAC, Mr. Friedman, on behalf of the Director, AFSA, made a presentation regarding this matter (Annex 2 to this Enclosure).

b. The minutes of the discussion at the AFSAC meeting form reference (b) to this report. The decision reached was as follows:

"DECISION: AFSAC authorized the Chairman to contact the Director, Central Intelligence with a view toward obtaining his views



OGA



together with a summary prepared by CIA (Annex 3 to this Enclosure).

c. On 16 February 1951, the Director, AFSA submitted preliminary comments

indicating specific points which should be amended or added, for purposes of further discussion in a second conference to be

The results of the conference are summarized in Annex 4 to this Enclosure.

~~U. S. EYES ONLY~~

ENCLOSURE "C"

8. a. On 9 March at the 61st Meeting of the United States Communications Intelligence Board (USCIB), a brief presentation of this subject was made for the information of the members of USCIB, by Mr. Friedman, on behalf of the Director, AFSA. No comments were made on the presentation. The minutes of the discussion at the meeting form reference (a) to this report.

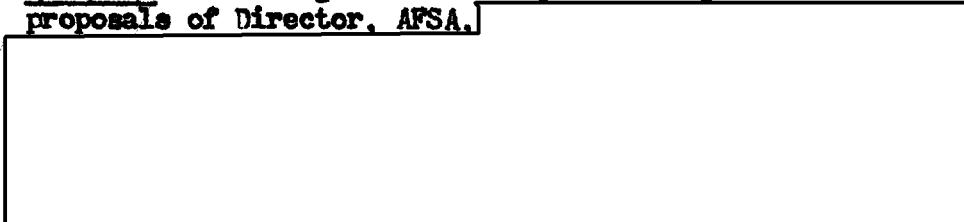
b. On 29 March 1951, the Director, AFSA submitted a Report on this matter to the members of AFSAC (reference (c)) and the memorandum was discussed at the 30th Meeting of AFSAC, on 6 April 1951. The minutes of the discussion form reference (d) to this report, a reading of which discloses that:

(1) Several members of AFSAC were doubtful of the advisability of making a deal which would cost \$700,000 and in which there was no



(2) Nevertheless, it was recognized that there was a possibility of reaping benefits [redacted] and, therefore, although AFSAC was unwilling to approve and thus to endorse the recommendations in AFSAC 66/20, it agreed as follows:

DECISION: AFSAC agreed to interpose no objections to the proposals of Director, AFSA.



9. a. On 6 April 1951, the Director, AFSA forwarded to the Director of Central Intelligence specific recommendations based upon a detailed study [redacted] referred to in Paragraph 7b above. A copy of these recommendations, which dealt principally with additional safeguards thought to be desirable for incorporation in the draft form, is attached as Annex 5 to this Enclosure.

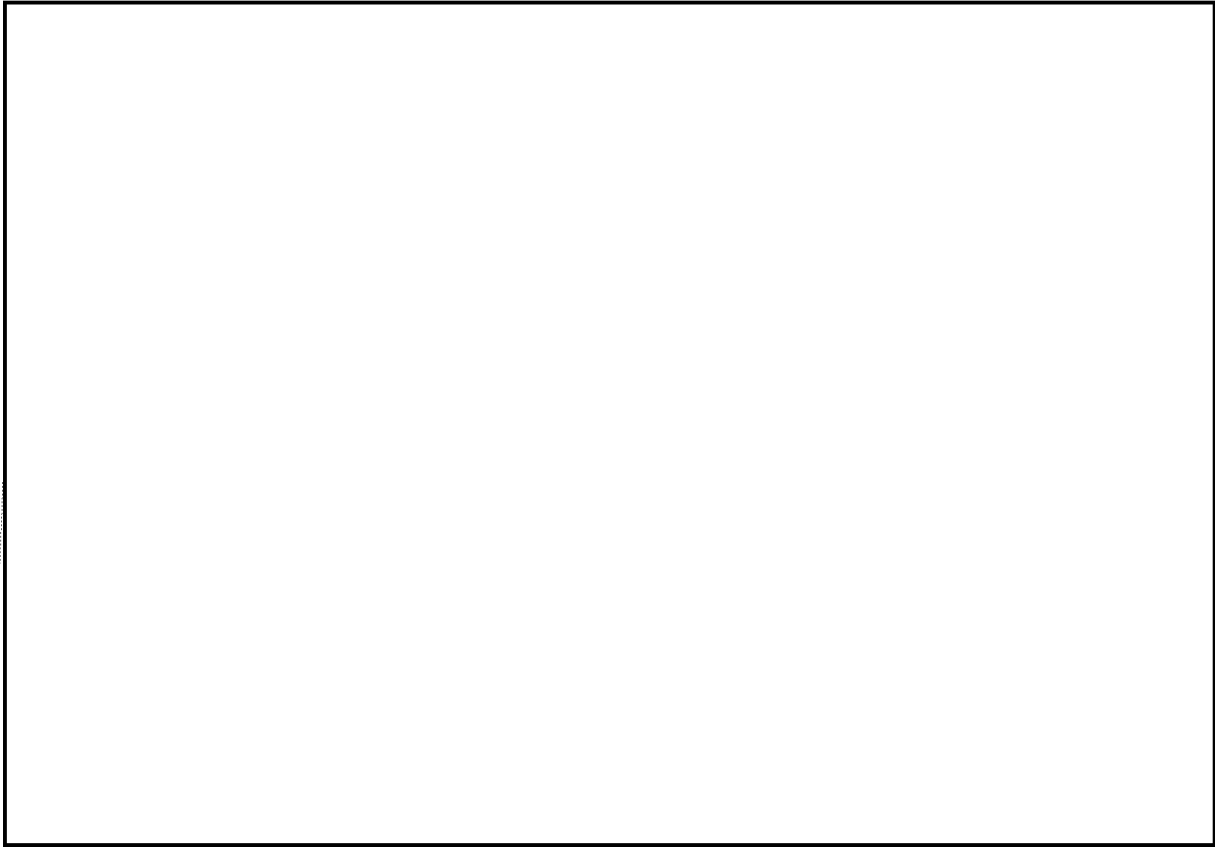
b. On 10 April 1951, the Director, AFSA forwarded to the Director of Central Intelligence a memorandum (see Annex 6 to this Enclosure) in which he summarized the broad considerations involved [redacted]

[redacted] and clarified his views concerning them.

~~U. S. EYES ONLY~~

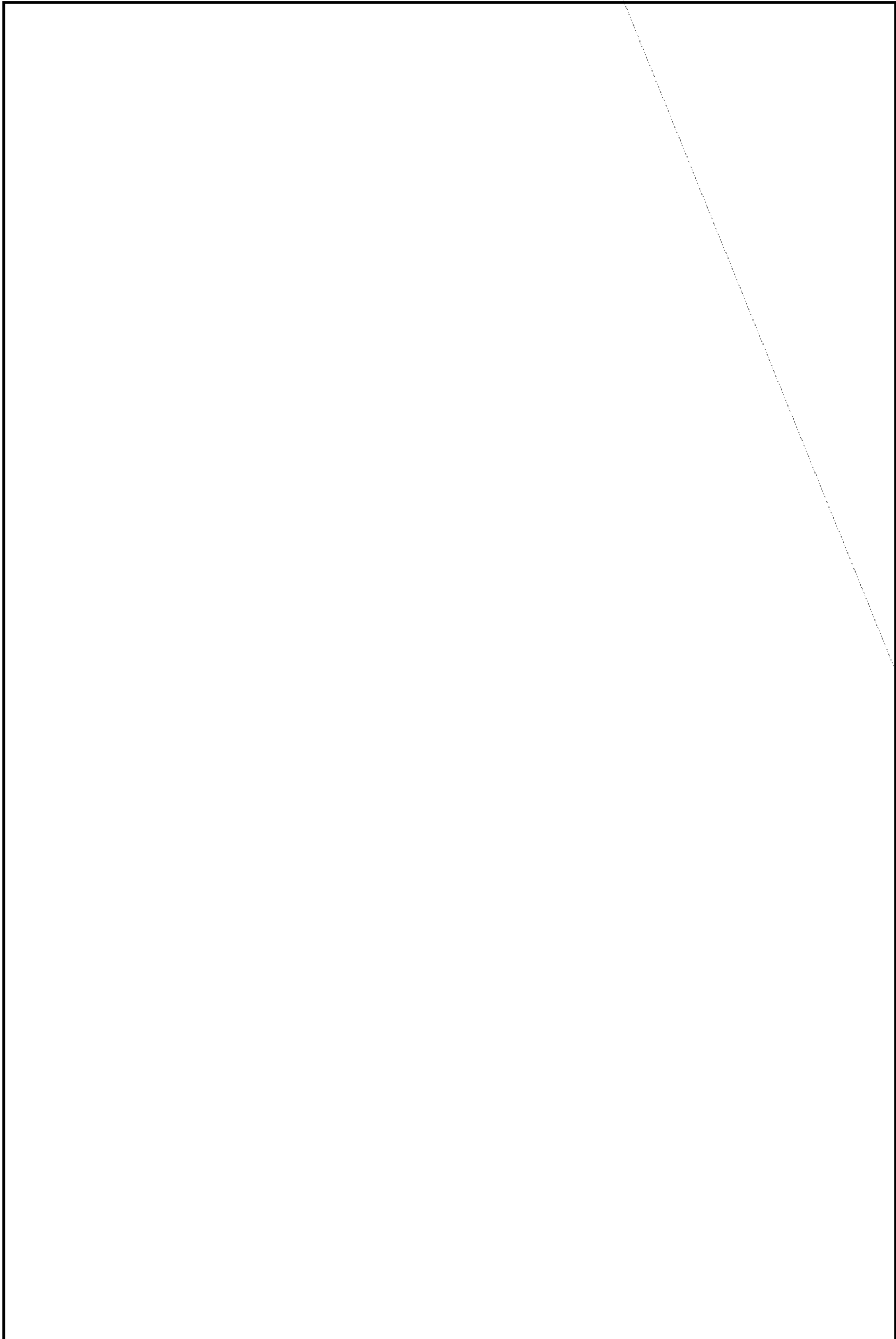
ENCLOSURE "C"

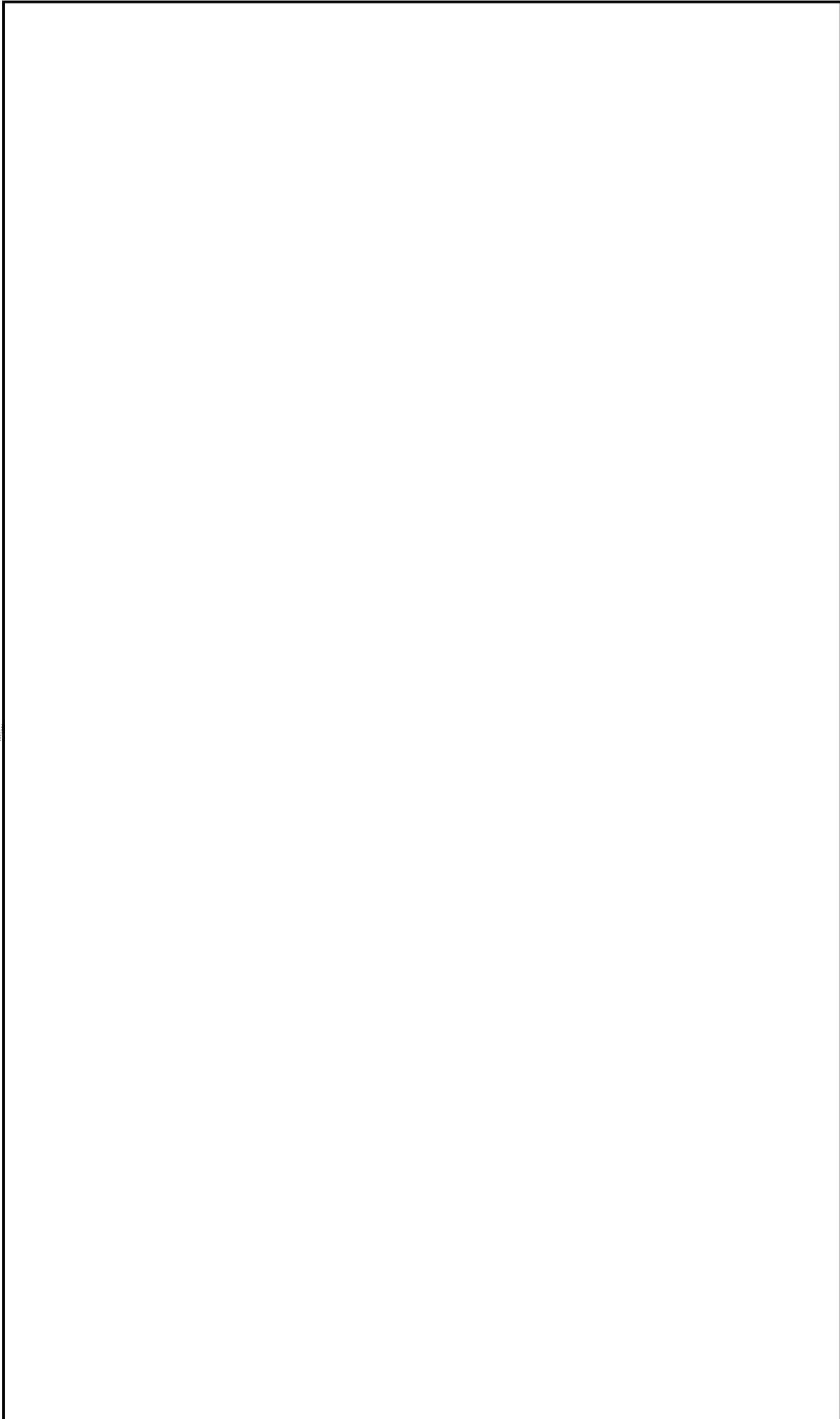
10.



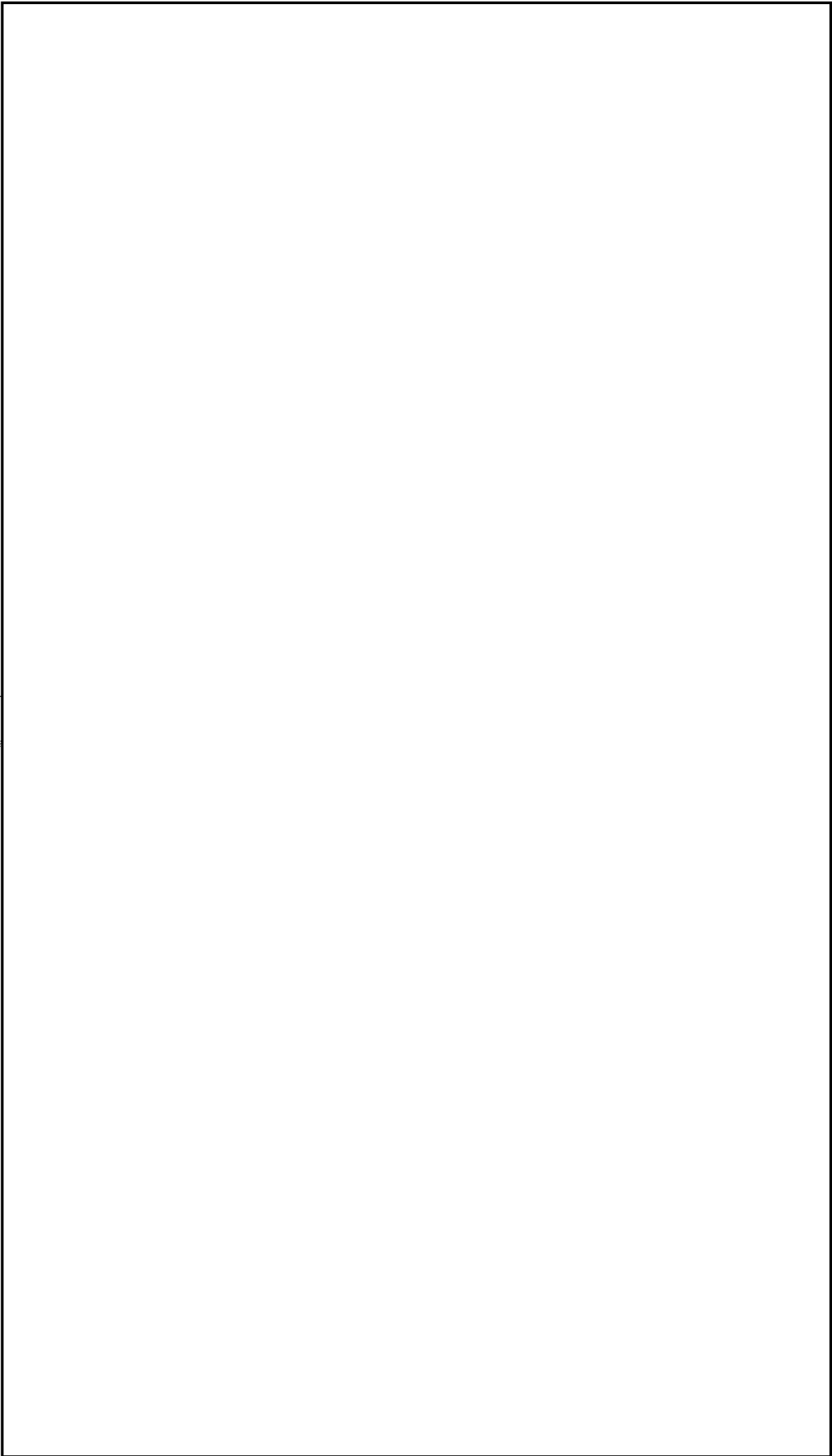
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Draft Memorandum of Agreement



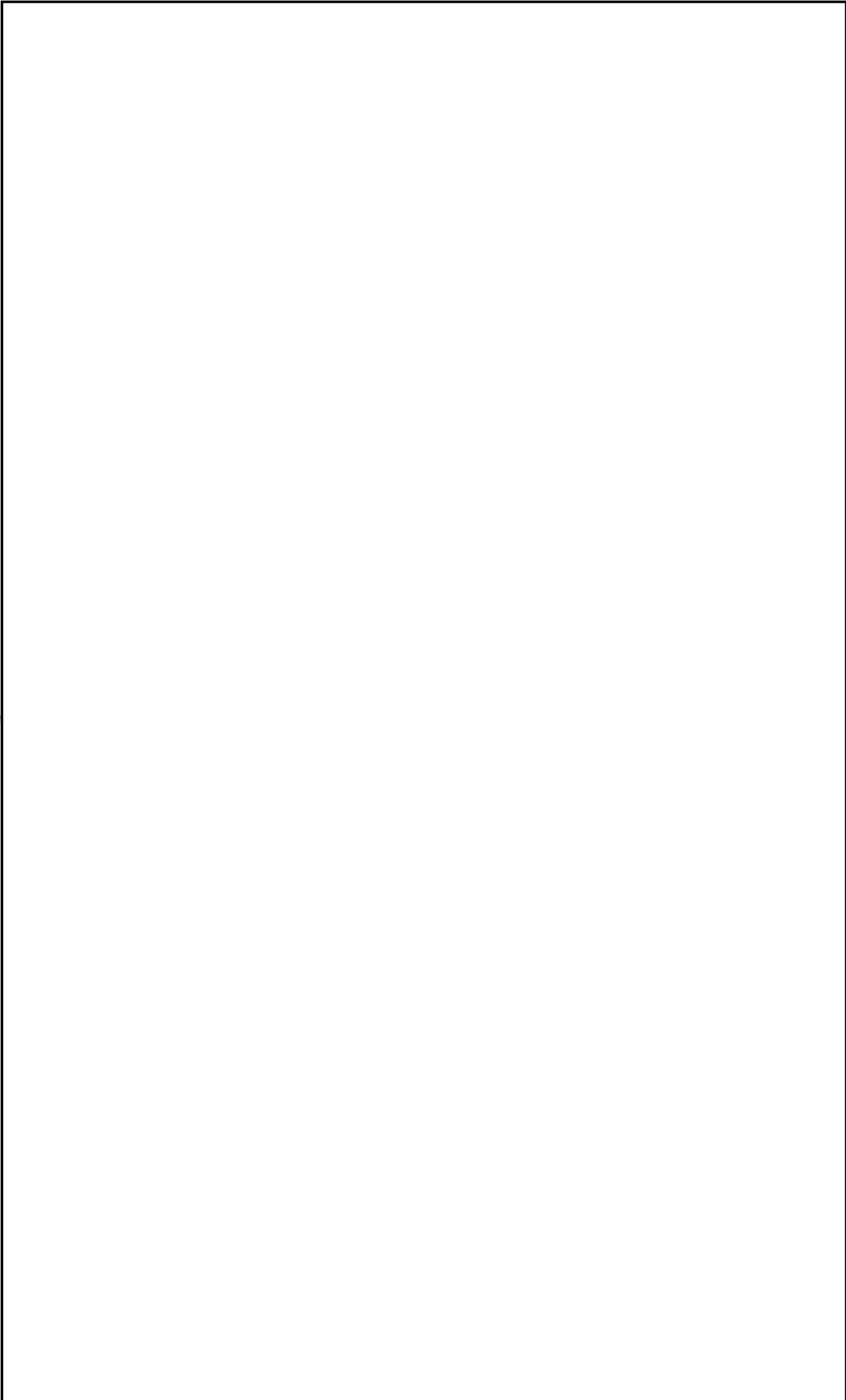


EO 3.3(h)(2)
PL 86-36/50 USC 3605



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

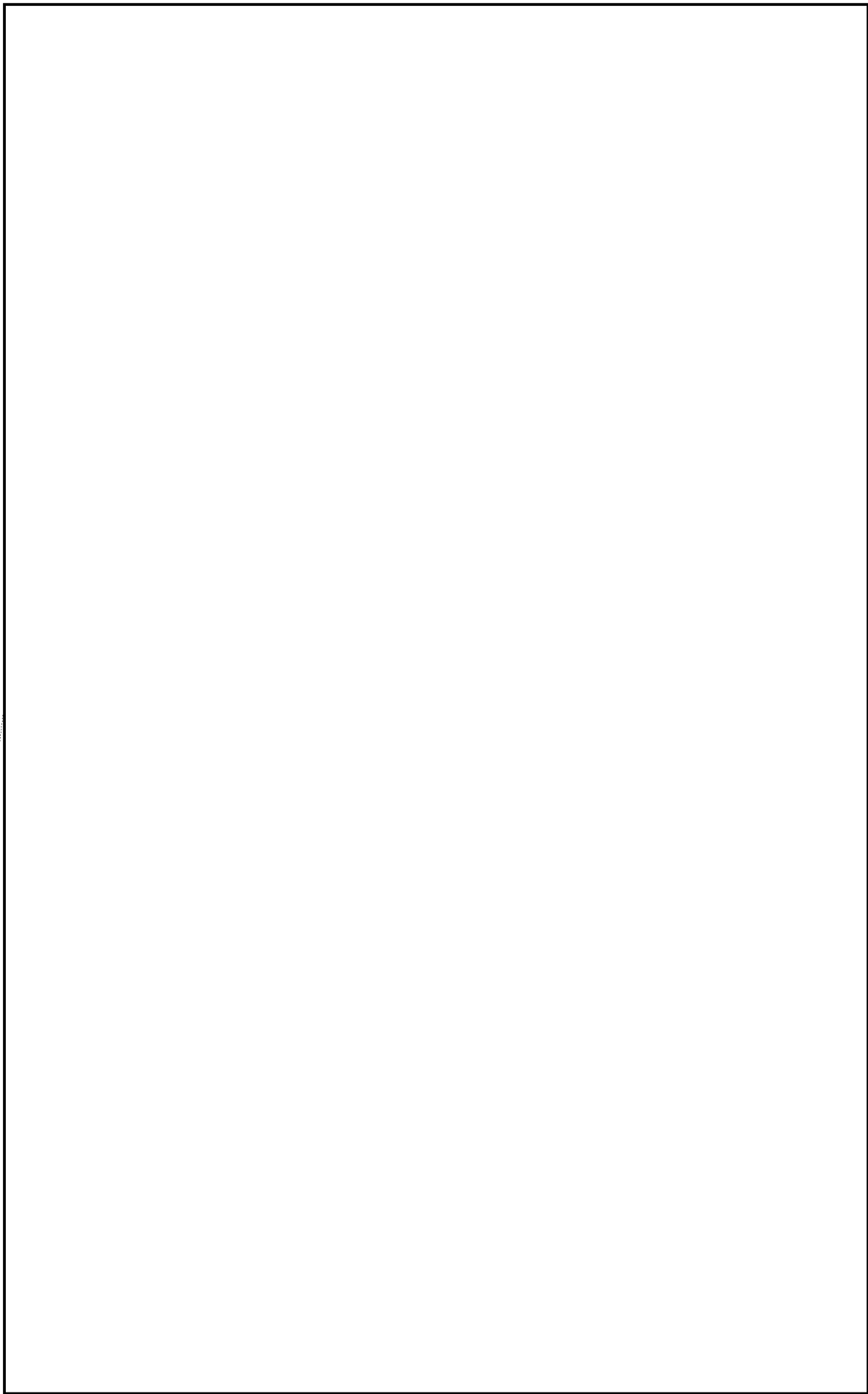
~~TOP SECRET~~



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

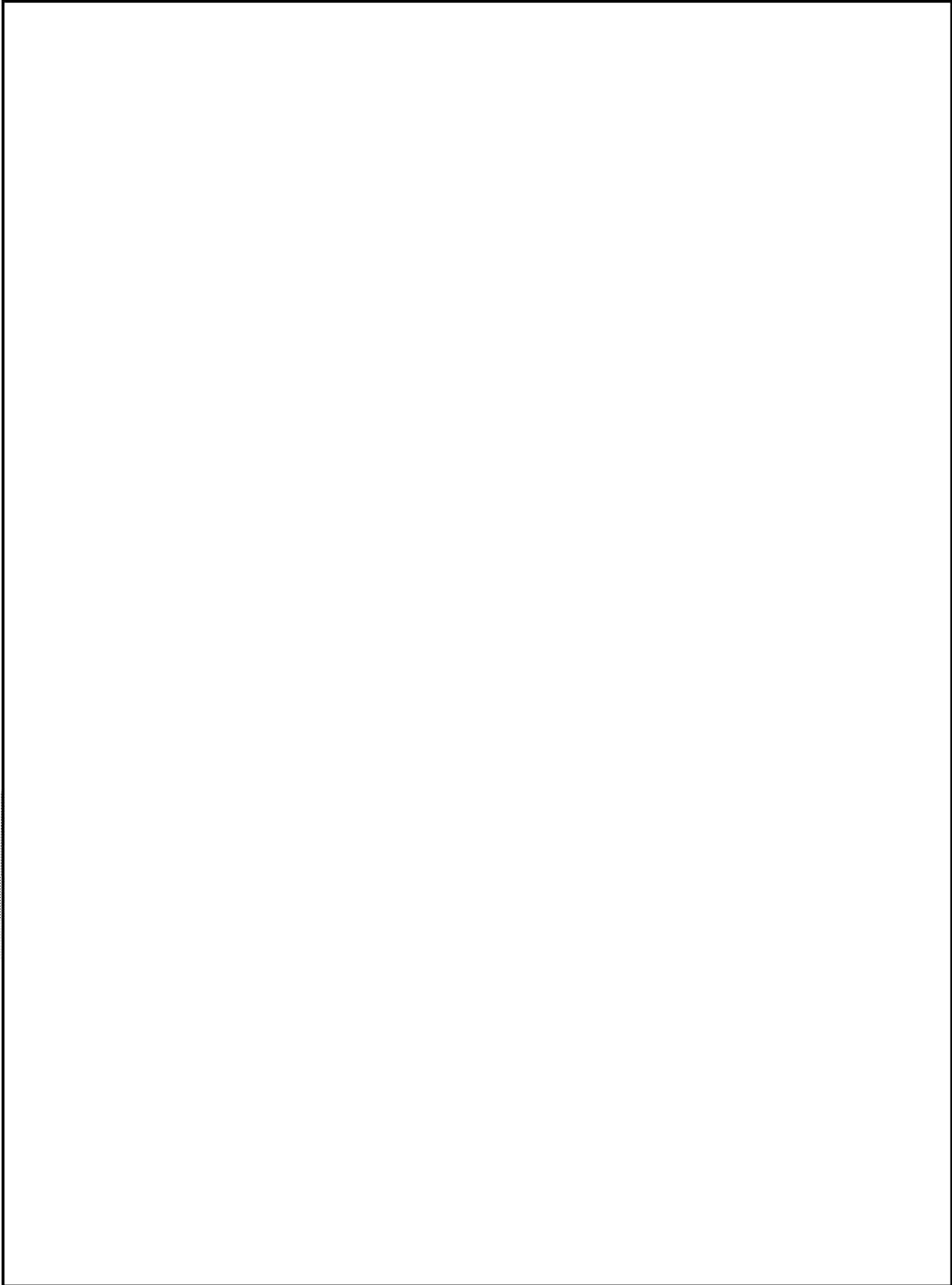
~~TOP SECRET~~

~~TOP SECRET~~



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

~~TOP SECRET~~



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