ALLIED FORCE HEADQUARTERS
OFFICE OF THE CHIEF SIGNAL OFFICER
APO 512, U. S. ARMY

X419

18 April 1944

SUBJECT: Fixed Call Signs.

TO: Chief Signal Officer, War Department, Washington 25, D. C.
Attn: SPSIS

Inclosed herewith for your information is a copy of memorandum on fixed call signs prepared by a member of the local YNA committee.

For the Chief Signal Officer:

R. E. SCHUKRAFT
Lt Col, Sig C

1 Incl:
Memo dtd 13 Apr 44, file B.389/753/6

If referred to by tele[illegible] please quote [illegible] 417

REF ID:A72356

~~TOP SECRET~~

ALLIED FORCE HEADQUARTERS
Office of the Assistant Chief of Staff G-2
SIGS I G-2 SECTION

B.389/753/6

13 Apr 44

Memorandum to: ADV
MI8
War Office
LONDON SW 1

Subject : Signal Security

1. A copy of Sigs 9 telegram No 85270 dated 8 April has been circulated to this section with regard to MIDEAST Manual of Signal Security.

2. Appendix B, which I submitted to X Branch, is characterised as an "Attack on War Office Policy governing Major Circuits". It seems that I should therefore put on record its origin and reasons.

3. The original MIDEAST Manual of Signal Security which is described as "excellent" in para 4 of telegram 85270 contains similar words at the beginning of the paragraph on fixed callsigns (c f chapter III para 5 "the system of allotting fixed callsigns to certain long range stations is inherently insecure") as the equivalent para in the printed Nov 1943 edition (chapter III para 5 " the system of allotting fixed callsigns to certain static WT stations working between and within commands is inherently insecure.").

4. During the visit by the S O in C to our station at [illegible], I mentioned the difficulty we are experiencing in recreating by traffic analysis diagrams of GERMAN networks and of sorting traffic, owing to the fact that the G[illegible] use changing callsigns for ALL their stations whether static or mobile, and constantly make changes devised to hinder the task of our interception service. I expressed the opinion that our methods seemed to be deteriorating since previously the use of fixed callsigns was restricted to the [illegible] ARMY CHAIN between commands and theatres, and now their use had been expanded to fixed stations.

5. I was subsequently asked to redraft para 5 of chapter III since the reasons justifying the statement that the system was " inherently insecure" were felt to be indifferently expressed. This I did and para 5 was altered and the Appendix B was added.

6. Chapter I para 4 of the Manual contains the following: "a distinction has been made between the procedures etc which SHALL be adhered to, and that which should be aimed at if circumstances permit in order to obtain as great a degree/of security as possible". If despite this, the repetition of the statement in the revised edition that the"system is inherently insecure" is regarded as an "attack on War Office policy governing major circuits" would it not be fair to suggest that the first duplicated edition which referred"to certain long range stations"contained the attack rather than the subsequent printed edition where the phraseology was changed to "workin between and within commands".

7. The Y intercommunication network has been directly affected by this expansion in the use of fixed callsigns. When the necessity for W/T links between SIGINT stations was first experienced, changing callsigns were allotted; now all our main stations including remote W/T stations use fixed callsigns. The size and activity of our Y strategical network is thus laid bare to the enemy.

~~TOP SECRET~~

8. For the reason given in para 7, and because I am convinced that it is my obligation to call attention to any apparent failure in our methods as compared with those adopted by the enemy, of which I become aware, I hope the question will be further considered.

9. I see that para 1 of 83270 Sigs 9 states that the MX arguments with reference to fixed callsigns are unsound. I have not had an opportunity of seeing the detailed reply to which reference is made.

10. The phrasing of para 5 and of Appendix B were not intended to be arguments, but reasons for the statement that the "system is inherently insecure" and so to encourage consideration of how far our signal security could be improved without prejudicing practical and speedy traffic disposal.

11. PRESENT ALLIED SYSTEM

I understand that our present ARMY system of callsigns allotment is

(i) all fixed stations, above the level of Army HQ, are allotted fixed four letter callsigns. They use double callsign procedure, thus clearly showing the originating and receiving stations.

Towns such as ALGIERS, CONSTANTINE, PHILIPPEVILLE (there are about thirty such allotments in NA and seventeen in ITALY) are given a fixed callsign and any WT station opening in that area uses that callsign, unless they have a special callsign which may then be used as a callsign or DG. In addition certain HQs or other units such as C in C MED, Adv MAAF, GHQ 2nd Echelon are given delivery groups composed of the same two first letters. These may appear in the preamble. Operational reserve units such as Corps HQs, Div HQs and units within a Division, AA units, Tank Bns although geographically behind Army HQ are allotted codesigns (changing daily).

(ii) all callsigns allotted to stations in a particular command or theatre start with the same two letters, and so are easily distinguishable from those of other commands

e.g.
- JA UK
- JB Americans in UK
- JC MIDMAST
- JD NORTH AFRICA
- JJ ITALY
- JP PERSIA
- JQ INDIA etc.

(iii) operational units are allotted daily changing callsigns, letters only (except for fig affixes below Bn level).

12. RAF use fixed callsigns, allotted to their HQs and Aerodromes. These do not change when one unit on an aerodrome replaces another.

When an advance takes place, and new aerodromes are opened, new callsigns are allotted. When an aerodrome ceases to be used callsign lapses.

I am told that the ME and NA callsigns can generally be distinguished; the former are composed of letter figure letter, the latter of figure figure letter.

The ground to air callsigns are not under discussion.

13. PRESENT GERMAN SYSTEM

(i) All stations with few exceptions, use daily changing callsigns composed of mixed figures and letters. They are usually used as link and not double callsigns.

(ii) GERMAN Airforce and GERMAN Army use the same type of high grade cipher, indistinguishable except by traffic analysis.

(iii) GERMAN Airforce and GERMAN Army book use the same callsigns in each book.

The exceptions mentioned in (i) are one or two highspeed links and some very low level units. The J callsign system seems to have discontinued, and contrary to our methods the use of fixed calls has been reduced rather than increased.

Recently it appears that the GERMAN Army and Airforce may be using the same book with different serials. In any case, their fear of disclosing any network, whether fixed or operational, is so great that they have taken and continue to take most drastic steps.

14. From the above description of the main differences between the BRITISH and GERMAN systems, it is possible to amplify the short summary of the reasons given for the inherent insecurity of our fixed callsign system.

15. <u>Chapter III para 5 of BRITISH Manual of Signal Security</u>

Each sub-para was amplified to some extent in the corresponding sub-para of Appendix B. It is impossible to summarise within a few words the extensive experience of the SIGINT organisation in studying the GERMAN networks or easy to make clear to anyone, not experienced in traffic analysis the extent of the knowledge which we present to the enemy as a gift.

16. Chapter III para 5, sub-para (a) "It simplifies the enemy's control over and the work of his intercept organisation". The difference between our Army and Airforce callsign systems enables him to allot the tasks to intercept units of the respective services without overlap.

The use of Army fixed callsigns with the first two letters clearly distinguishing the area where the transmitter is situated, and enables him without difficulty

(i) to compile and maintain accurate diagrams of all our fixed networks. The double callsign procedure helps considerably;

(ii) to direct his intercept stations to the tasks allotted without difficulty and to eliminate what is not wanted at that station;

(iii) to distinguish rapidly and without assistance of DF the creation of new WT stations in areas thus disclosing concentrations, movements by land or sea etc.

17. It may be suggested that it does not matter facilitating the "enemy's control over and work of his intercept organisation" provided he does not gain by it. Can he fail to do so? Without any success in cryptography at all, I suggest that our present system cannot avoid giving him <u>early indications of intentions</u>, which may be confirmed or confirm information from other sources.

18. <u>ESTIMATION OF OUR RESERVES, AND THEIR LOCATION</u>

The use by Divisions and certain other units of codesigns (daily changing) though temporarily located geographically behind ARMY HQ will enable the enemy to discover

(i) the general area in which reserves are located
(ii) their size, comparative to previous records
(iii) the arrival of new formations
(iv) major moves.

The use by CD and AA units of codesigns in the same area will similarly

enable them to estimate concentrations and observe moves.

Any change in the "codesign - fixed callsign junction point" of the above will assist, and also probably reveal changes of subordination. The number of messages that require retransmission between a Corps or Div H.Q. in reserve and during refitting, to higher formation H.Q. is probably higher than when operationally employed.

19. The use of fixed callsigns for Ports, Railheads, important towns, Districts and billeting areas will tend to give similar information in view of the inevitable changes in the volume of traffic, consequent on concentrations or departures.

The allotment of additional fixed callsigns to towns or other stations, and the lapsing into silence and non-use of others will also provide information of infiltration and increased or decreased concentrations. The existence of BRITISH AT stations in TURKEY was mentioned by an ITALIAN cryptographer and was probably disclosed by the use of JC callsigns of new stations communicating with CAIRO (JCJC).

The GERMAN Police used to use fixed callsigns. In 1941, the GERMAN infiltration into ROUMANIA was spotted as a result of this, and caused search to be made for Army stations using changing callsigns in that area. Owing to the inaccuracy of D/F and the difficulty of the callsign procedure, this search was not conclusive but confirmatory.

We are aware from captured documents that GERMAN intercept stations render a daily return of formations or units subordinated to senior formations. This assists their records of our Order of Battle. Our callsign system facilitates this.

There are probably other compromises of direct military value, based on the background knowledge acquired by persistent interception and traffic analysis.

20. Chapter III para 5 sub-para (b) "It provides aids to enemy cryptographic attack on cipher traffic".

There can be no doubt that the enemy has a large cryptographic organisation. Unless our high grade machine and book ciphers are absolutely secure, ~~the fact that~~ our codesign system enables him CALL

(i) to determine the originating station and the receiving station without doubt from day to day of each message;

(ii) to sort all traffic accordingly;

(iii) to follow the course of re-transmitted messages and from the T or DG instruction in the prefix to try out possible re-transmitted re-enciphers of the same message.

If a message addressed from a station within the fixed callsign area to a station in the daily changing codesign zone is not re-enciphered, the changing codesign is compromised with the fixed callsign and possibly from day to day. I gather that shortage of cipher staff renders this latter callsign compromise inevitable. The alternative seems to be two cipher versions of one message.

21. The system seems to facilitate enemy cryptographic attack in that

(i) any indiscretion and compromise can be worked on

(ii) routine messages can be collected from day to day;

(iii) captured files of telegrams or cipher documents can be examined against earlier cipher traffic intercepted.

22. The present system presents fewer difficulties than the "old wave code callsign system" where each terminal at a large station had a different callsign. In the summer of 1941, the writer with two receivers and one NCO produced a diagram of MIDEAST static stations in the area CYPRUS, SYRIA, PALESTINE, EGYPT, and SUDAN when the wave code system was in force.

23. Corroboration of the above statements comes from prisoners and co-belligerent ITALIANS. The latest arrival "ARNOLD", ref SIXT/MR/359, was employed for 4 weeks only on low grade traffic classification, and as a teleprinter operator. The ease with which enemy intercept is controlled is shown by the organisation of the service into 8 REGAIONE, No 4 at BELGRADE being responsible for BALKAN area, No 7 for ITALY.

24. No 4 REGAIONE has

HQ at BELGRADE (20 watches)
Intercept station No 5 at SALONICA (30 watches)
" " No 6 at ATHENS (30 watches)
Mobile Intercept Coy with HQ PACK 2
3 D/F stations.

25. The prisoner worked at No 6 intercept station at ATHENS, and states that all types of traffic analysis and cryptanalysis are done there. His opinion was that BRITISH Signals Security was poor, that groups using fixed callsigns are particularly easy to intercept. He said that JOJO (CAIRO) was treated as a priority. The full report (SIXT/MR/359 dated 4 Apr 44) is worth reading.

CONCLUSION

26. It is difficult to explain to anyone not versed in traffic analysis the results that can be achieved.

In the Appendix there are imaginary reports from the GERMAN intercept station at ATHENS

(i) for the year 1944 whilst BRITISH used fixed callsigns

(ii) and (iii) for two successive weeks in 1945 after a change to daily changing callsigns.

It is hoped perusal of these may assist.

27. The practical difficulties of adopting changing callsigns to fixed networks are said to be great, if delay in routing traffic is not to result. The GERMANS, however, overcame this. An up to date analysis of their callsign methods and traffic routing from OKW might solve the problem.

28. Compromise of callsign books used by operational units could be overcome by the provision of a new book for fixed stations. If well designed, a very long time would elapse before the enemy could reconstruct it, particularly if all figures as well as letters were used throughout.

I suggest that the SIGINT staff working on GERMAN traffic obtains a very full insight into the interrelation of signal and cipher security and of what forms of RT procedure are insecure or secure. May I suggest that the officers of Sigs 9 confer with SIGINT officers doing traffic analysis, on the subject.

A Tojer.

A. TOJER,
Colonel, G.S.

Copy to: CSO AFHQ
S O in C MIDEAST

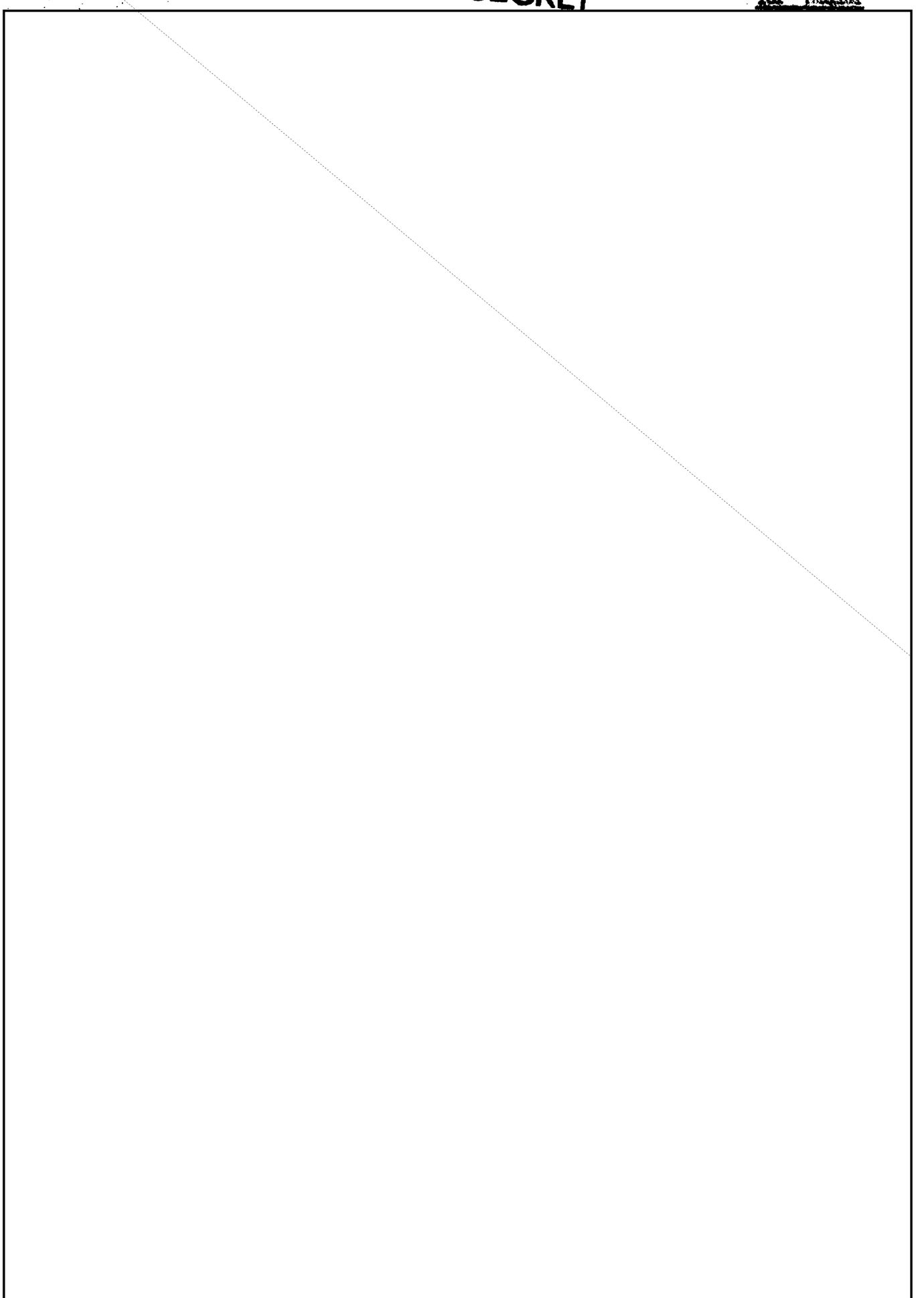
6

7. [redacted] - Diagram of [redacted] Railway [redacted] Junction.

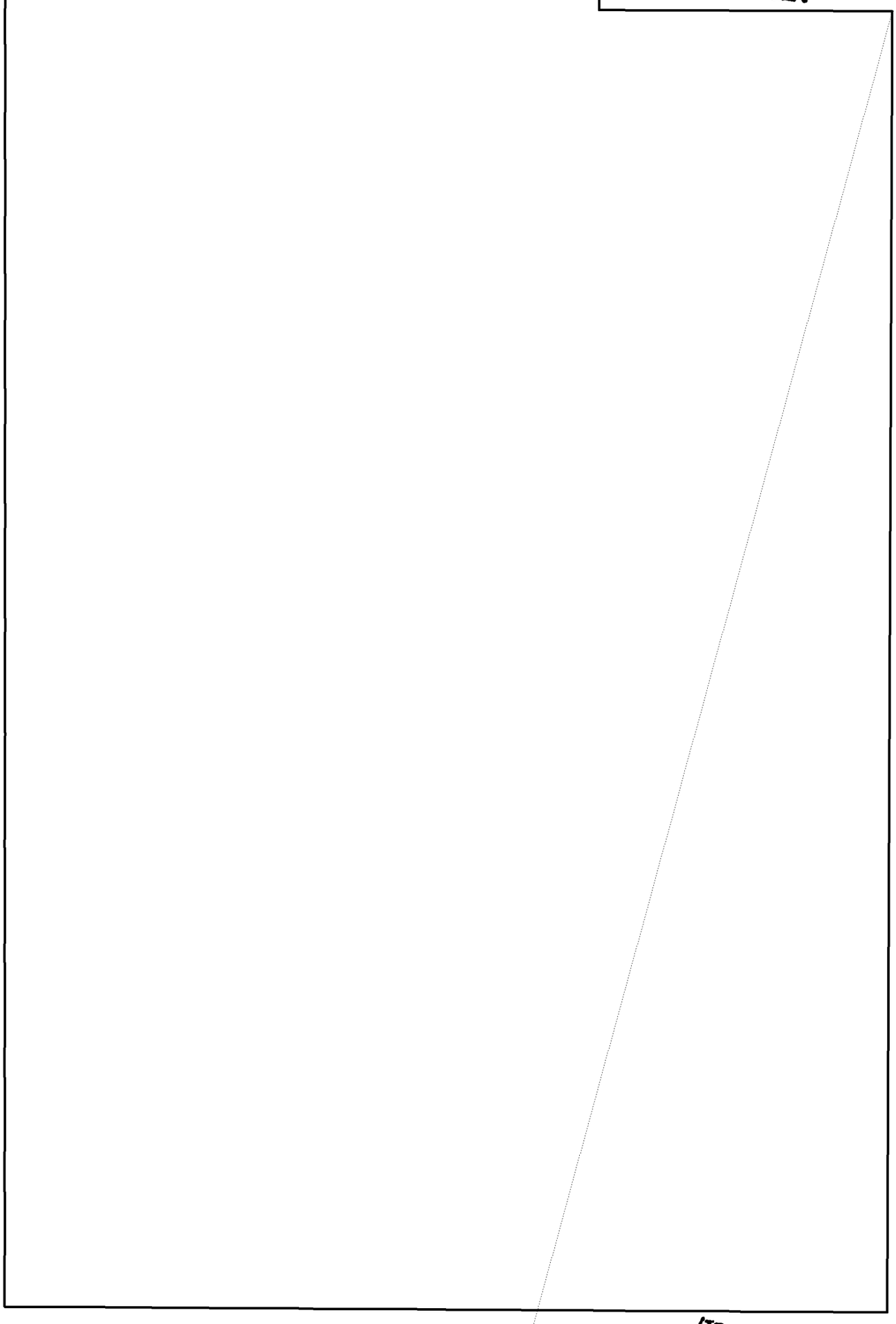
REF ID:A72356

TOP SECRET

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

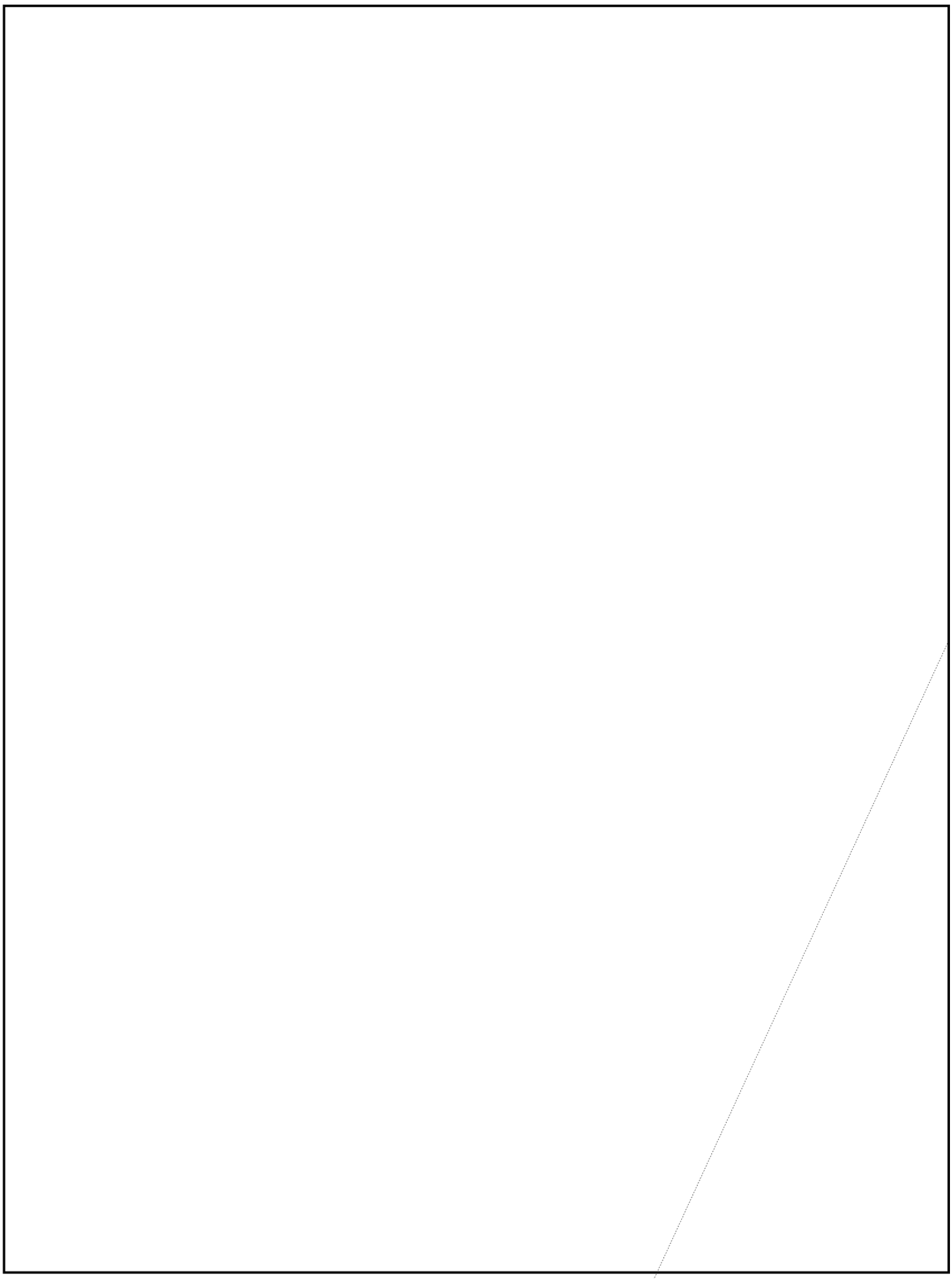


~~TOP SECRET~~



/In .....

~~TOP SECRET~~



12