

REF ID: A72356
~~TOP SECRET~~

~~SECRET~~
By Authority of
C-in-C., A.F.

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

Initials *ES*

Date *18/4/44*

18 April 1944

X419

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:

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

R. E. Schuckraft
R. E. SCHUCKRAFT
Lt Col, Sig C

Declassified and approved for release by NSA on 01-26-2015 pursuant to E.O. 13526

~~TOP SECRET~~

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

B. 389/753/6

13 Apr 44

Memorandum to: JCY
MIS
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 MIBAST Manual of Signal Security.
2. Appendix B, which I submitted to X Branch, is characterized 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 MIBAST 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 call signs (of chapter III para 5 "the system of allotting fixed call signs 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 call signs to certain static ST stations working between and within commands is inherently insecure.").
4. During the visit by the S O in C to our station at HENNINGHAM, I mentioned the difficulty we are experiencing in recreating by traffic analysis diagrams of GERMANY networks and of sorting traffic, owing to the fact that the GERMANS use changing call signs 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 call signs was restricted to the MAIN 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/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 call signs. When the necessity for Y links between SIGS stations was first experienced, changing call signs were allotted; now all our main stations including remote ST stations use fixed call signs. The size and activity of our Y strategical network is thus laid bare to the enemy.

~~TOP SECRET~~

of security

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 BIZTO sign 9 states that the MI arguments with reference to fixed callsigns are unavailing. 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. ARMY ALLIED FORCE

I understand that our present Army system of callsign 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.

Units such as ALGERIA, CONSTANTIN, PHILIPPEVILLE (there are about thirty such allotments in MA and seventeen in ITALY) are given a fixed callsign and any OT station operating in that area uses that callsign, unless they have a special callsign which may then be used as a callsign or DC. In addition certain HQs or other units such as C in C MED, Adv MAAP, GHQ and Subdivs 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 callsigns (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
	JO	MIDWAY
	JD	NORTH AFRICA
	JJ	ITALY
	JF	FRANCE
	JB	INDIA etc.

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

12. RAF use fixed callsigns, allotted to their HQs and Aerodromes. These do not change when one unit or 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 MA and MI 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. ARMY ALLIED FORCE

(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.

~~TOP SECRET~~

- (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 both use the same ciphers in each book.

The encryptions mentioned in (I) are not or two keyperiod links and some very low level units. The 3 cipher system seems to have eliminated, and conformity to our methods the use of fixed ciphers has been reduced rather than increased.

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

From the above description of the main differences between the ~~WIRING~~ and GERMAN systems, it is possible to supply the short summary of the reasons given for the inherent insecurity of our fixed cipher system.

15. CHAPTER III, para. 1, of JMWAVE Manual of Signal Security

Each sub-group was supplied to know extent in the corresponding sub-group of Appendix B. It is impossible to summarize within a few words the extensive experience of the STRIDY organization in studying the GERMAN methods or easy to make clear to anyone, not experienced in traffic analysis the extent of the knowledge which we possess to the enemy as a gift.

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

The use of Army fixed ciphers with the fixed one letter's cipherly 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 cipher procedure helps considerably;
- (II) to forward his intercept stations to the units allotted without difficulty and to indicate what is not worked at that station;
- (III) to distinguish rapidly and without encumbrance of IP the location of new IP stations in areas thus distinguishing 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 organization" 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 early indications of intentions, which may be confirmed or confirm information from other sources.

18. ESTIMATION OF OUR RESERVE, AND THEIR LOCATION

The use by Divisions and certain other units of ciphers (daily changing) through temporarily located geographically located AMRT 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 ciphers in the same area will similarly

~~TOP SECRET~~

4

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 Hq, in reserve and during refitting, to higher formation Hqs 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 JG callsigns of new stations communicating with CAIRO (JGJC).

The GERMAN Police used to use fixed callsigns. In 1941, the GERMAN infiltration into ROMANIA 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/P 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, ~~we must~~ ^{we can} our ~~callsign~~ ^{callsign} system enables him

- (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.

~~TOP SECRET~~

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 M20 produced a diagram of MIDEAST static stations in the area GYTHUS, SYRIA, PALESTINE, EGYPT, and SUDAN when the wave code system was in force.

23. Confirmation of the above statements comes from prisoners and co-belligerent ITALIANS. The latest arrival "ARNOLD", ref SINT/AG/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 organization of the service into 8 BUREAUX, No 4 at BELGRADE being responsible for BALKAN area, No 7 for ITALY.

24. No 4 BUREAU has

HQ at BELGRADE (20 watches)
Intercept station No 5 at SALONICA (30 watches)
" " " " No 6 at ATHENS (30 watches)
Mobile Intercept Coy @ HQ PACK 2
3 D/V 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 (SINT/AG/359 dated 4 Apr 44) is worth reading.

CONCLUSION

26. It is difficult to explain to anyone not versed in traffic analysis the results ^{etc} 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, overcome this. An up to date analysis of their callsign methods and traffic routing from GCHQ 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 WT procedure are insecure or secure. May I suggest that the officers of Sign 9 confer with SIGINT officers doing traffic analysis, on the subject.

A. F. Jones

A. F. JONES,
Colonel, G.S.

Copy to: GSO AFHQ

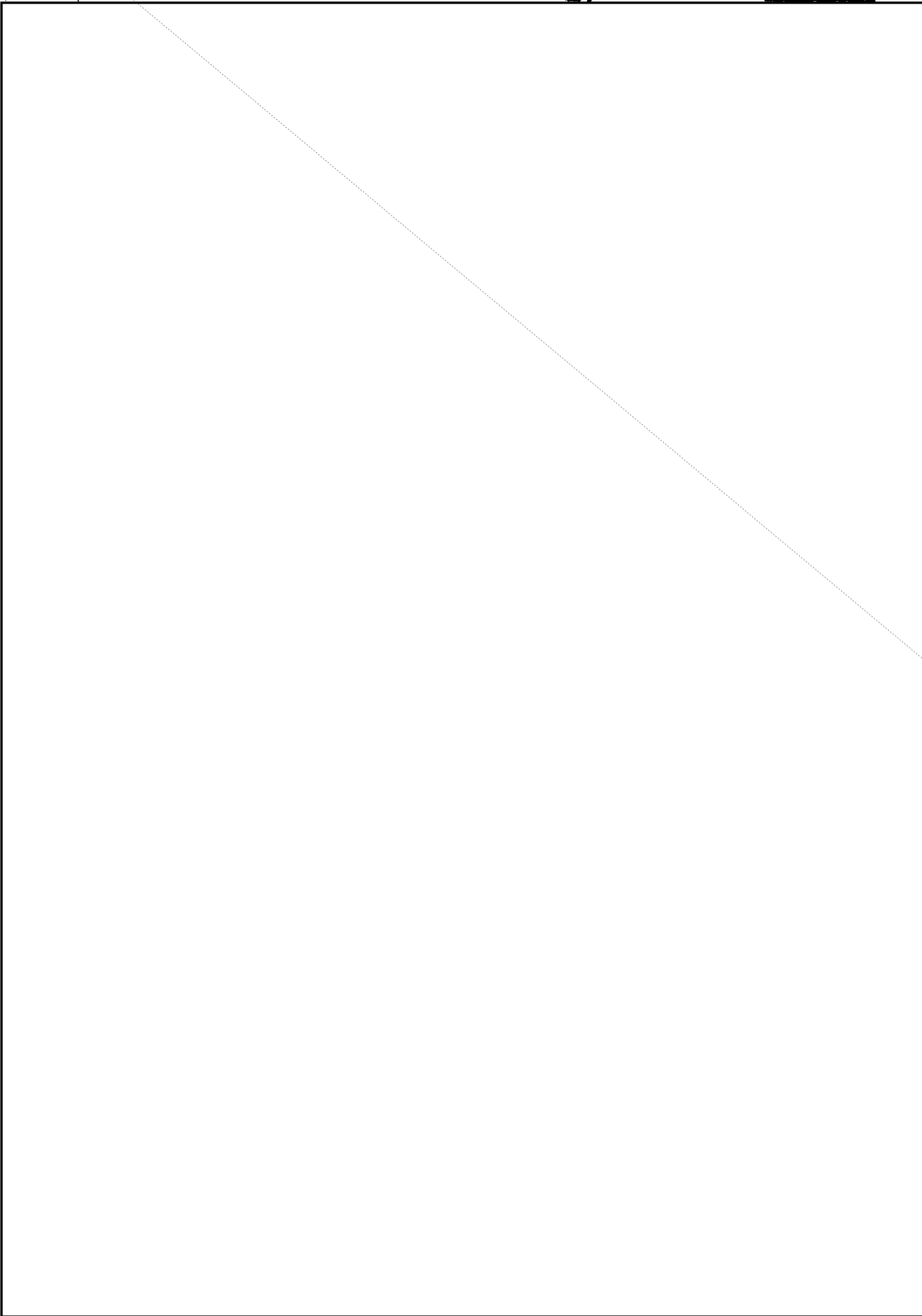
S O In G MIDEAST

~~TOP SECRET~~

8
~~TOP SECRET~~

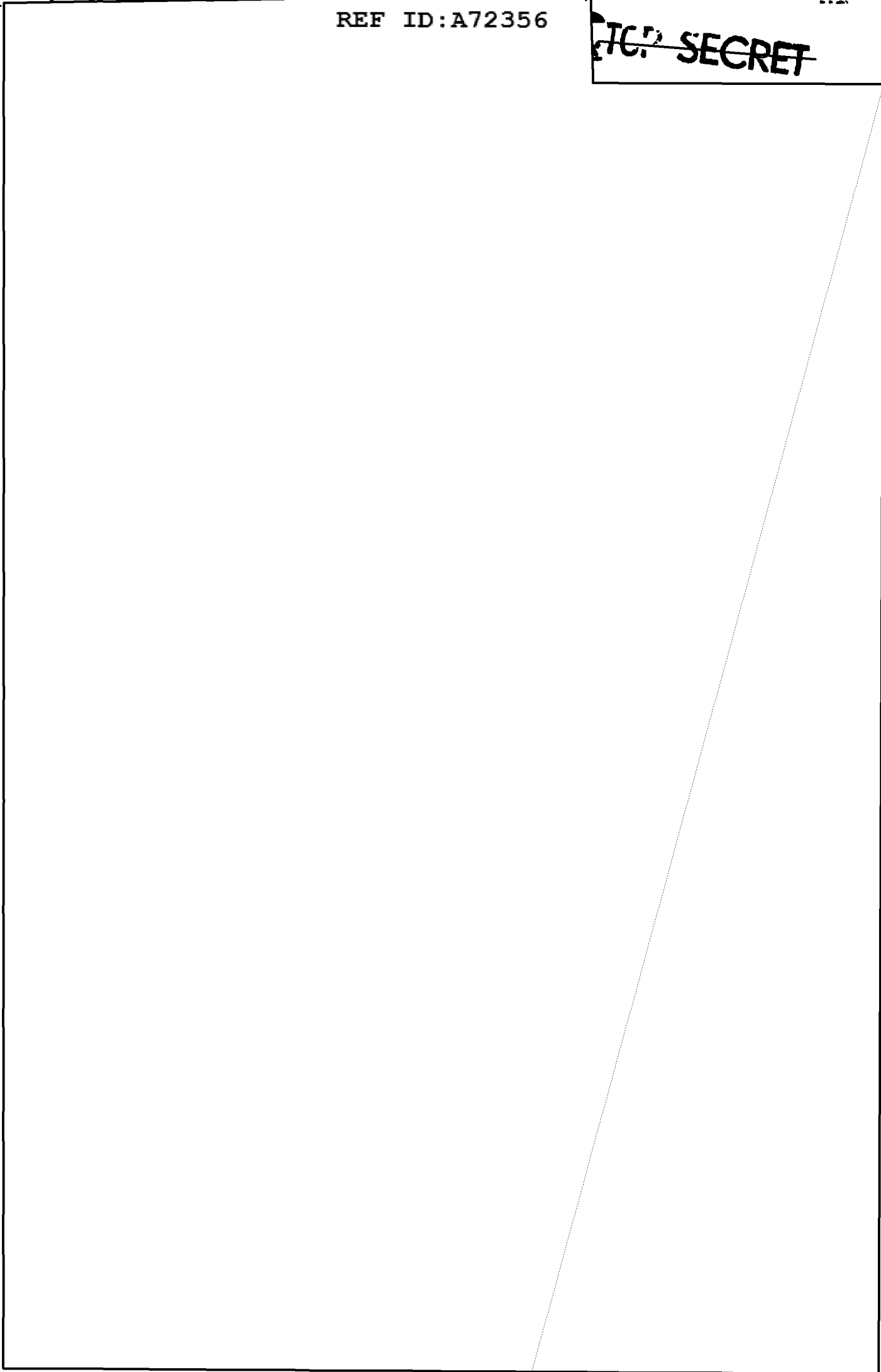
~~TOP SECRET~~

~~TOP SECRET~~



~~TOP SECRET~~

~~TOP SECRET~~

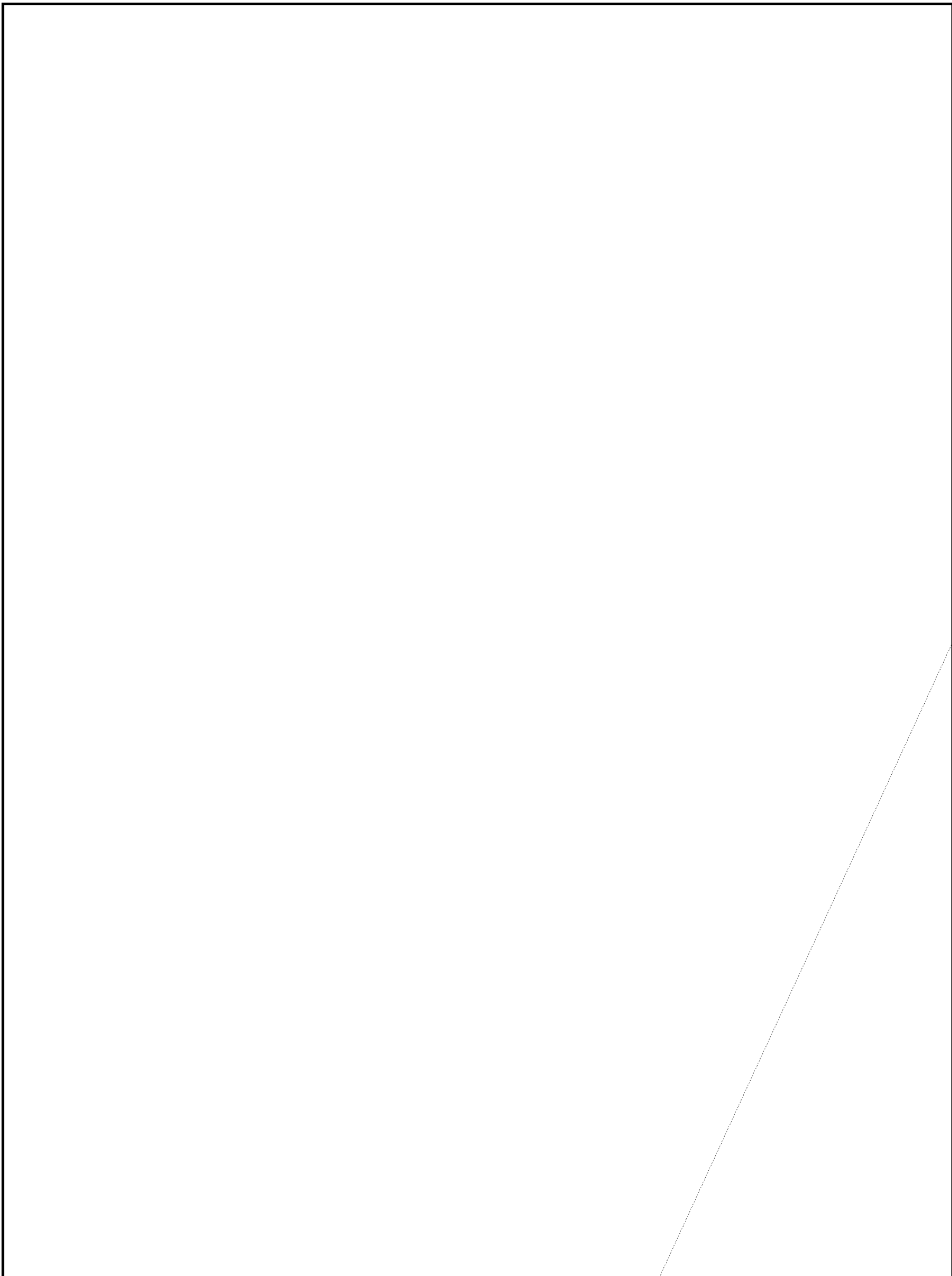


/s/

~~TOP SECRET~~

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

~~TOP SECRET~~



~~TOP SECRET~~

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

12