

MEMO ROUTING SLIP

REF ID: A55669

NEVER USE FOR APPROVALS, DISAPPROVALS,
CONCURRENCES, OR SIMILAR ACTIONS

| | | | |
|---|---|-------------------------|------------------|
| 1 | NAME OR TITLE <i>Capt Mason</i> | INITIALS | CIRCULATE |
| | ORGANIZATION AND LOCATION <i>AFSA-02</i> | DATE | COORDINATION |
| 2 | | | FILE |
| | | | INFORMATION |
| 3 | | | NECESSARY ACTION |
| | | | NOTE AND RETURN |
| 4 | | | SEE ME |
| | | | SIGNATURE |
| REMARKS | | | |
| <p>1. This has been coordinated, ^{with} and reviewed by Dyer, Peterson, and Wenger. It is desired that you review it and add anything you deem pertinent, or change anything you deem necessary.</p> <p>2. Please check figures in Par. 9a(3) of discussion & add any other similar data which might be significant.</p> | | | |
| FROM NAME OR TITLE <i>Friedman</i> | | DATE <i>6 Nov 50</i> | |
| ORGANIZATION AND LOCATION <i>001</i> | | TELEPHONE | |

FORM NO 95
1 OCT 48Replaces DA AGO Form 895,
1 Apr 48, which may be used.

16-45197-8 ☆ CPO

REF ID: A55662
~~TOP SECRET ACORN~~

COORDINATOR, USCIB
REPORT BY THE DIRECTOR, ARMED FORCES SECURITY AGENCY
TO THE UNITED STATES COMMUNICATIONS BOARD

~~via~~

~~THE ARMED FORCES SECURITY AGENCY COUNCIL~~

on

MEASURES FOR INCREASED SECURITY OF COMMUNICATION INTELLIGENCE

THE PROBLEM

1. What additional measures should be taken to protect such COMINT sources as may be expected soon to yield vital information, the drying up of which should be prevented at all costs?

FACTS BEARING UPON THE PROBLEM AND DISCUSSION

2. As set forth in Paragraphs 1-12 in the Enclosure.

CONCLUSIONS

3. It is concluded that:

a. A review of the entire problem of COMINT security is warranted in the light of the present situation wherein there appears to be a gradual lessening of security in the face of a more pressing need therefor.

b. The possibility of some approach to a state of readability of certain high-level cryptosystems makes it imperative that there be no delay in the re-examination of present COMINT security measures and the formulation and application of new or additional measures which may prevent a repetition of the losses suffered in the recent past.

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

c. In connection with certain current high-level COMINT problems it is possible and it may be advisable to institute security safeguards such as were in force in connection with certain high-level COMINT problems in World War II.

RECOMMENDATIONS

4. It is recommended that:

a. USCIB direct the USCIB Security Committee to make the review referred to in Par. 3a and to submit recommendations arising from a consideration of Pars. 3b and 3c of the foregoing conclusions.

b. The USCIB Security Committee be directed to submit its report to USCIB not later than 15 December 1950.

~~TOP SECRET ACORN~~

~~TOP SECRET~~~~ACORN~~
ENCLOSUREEO 3.3(h)(2)
PL 86-36/50 USC 3605FACTS BEARING UPON THE PROBLEM AND DISCUSSION

1. The Director, AFSA is becoming increasingly concerned over what appears to be a gradual lessening of the security of COMINT in the face of a more pressing need therefor. Although a number of important and basic steps have been taken since the war to establish security on a firmer foundation, other developments have occurred which have, to a large extent, nullified the effects of our advances.

2. Since the end of World War II there has been a continual improvement in the types of cryptosystems employed by foreign governments and a steady tightening of communication security practices, especially by the [redacted]. Not only has this been true, but even when as a result of concentrated effort AFSA succeeded in solving these ^{certain [redacted] cryptosystems,} ~~communications,~~ the fruits thereof were soon denied us because of the withdrawal from usage of all [redacted] high-level systems soon after success in their solution was attained.

3. Of the types of high-level systems still in use by [redacted] one is unreadable and the other has been read fragmentarily to a very limited degree. In the latter case, work has been surrounded by the most stringent safeguards and virtually no dissemination has been made of end products.

4. Meanwhile there has been a steady and substantial increase of both workers and consumers. ^{list of consumers alone} The indoctrinated ~~list~~ has risen from 584 in February 1947 to 1,332 in June 1950. In addition, there have

~~TOP SECRET~~~~ACORN~~

~~TOP SECRET ACORN~~

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

been innumerable individuals brought into the fringe of knowledge for administrative, budgetary, or other reasons.

5. Aside from the foregoing, certain dissemination safeguards have gradually been relaxed. Material is now distributed and maintained in a number of areas in Washington outside the producing agencies, where it was never permitted before. Moreover, distribution has been authorized to additional agencies. Restrictions on the distribution of material to, and maintenance in, occupied areas have also been eased.

6. In the face of all this, the demand for COMINT has become increasingly great and the need for its protection imperative. We have now been virtually out of touch with high-level communications for three years. If we should regain contact and then lose it again we are likely to be denied this vital source of intelligence for a much longer period.

7. Since the War, the basic essentials for effective security control have finally been established after years of effort. We now have:

- a. A federal protective law
- b. Security agreements with our foreign collaborators
- c. Improved investigative machinery
- d. An interdepartmental authority (USCIB)
- e. Common security standards
- f. A single U.S. producer of high-level COMINT (AFSA)
- g. General appreciation of the value of COMINT

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

8. In addition to the foregoing, there has been instituted within AFSA itself a fairly rigid system of compartmentation of problems, a feature which militates against technical efficiency, ^{in COMINT production} but which is considered essential for security.

9. a. ~~However,~~ ^{Despite} the mechanisms and factors listed above, it is not believed that the security situation has been improved to a degree which warrants brushing aside of all fear that further or future success on high-level problems may be nullified by leakage of information to the Governments whose communications have been successfully attacked. In fact, the basis for continued apprehensions on this score remains the same, or even stronger than before because of certain shortcomings in the COMINT security picture. Among them are the following:

(1) ^{Possibly} ~~too~~ much individual authority and discretion are left to individual consumer and producer agencies to insure uniform application of adequate security measures. (The security control of atomic energy information is more centralized and rigid.)

(2) There is no over-all authority to insure observance of security regulations. (Inspection authority such as that which was exercised by the Cryptographic Security Board might well be vested in USCIB.)

(3) ~~There is far too wide~~ ^{The} dissemination of results. ^{is much too voluminous for safety} (Over 1,000,000 copies of COMINT translations, representing some 16,000 individual decrypted messages, were disseminated in September, 1950. The handling of the German problem proved that COMINT can be effectively used even with the most drastic restrictions on dissemination.)

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

(4) The administrative, control, and budgetary machinery and procedures are such that large numbers of individuals must be apprised of numerous details of COMINT activities. (The large number of agencies, offices, boards, and committees concerned with the operation and administration of COMINT activities necessitates innumerable reports, justifications, etc., which are very hazardous to security. The arrangements governing the operation of CIA are much more conducive to secrecy.)

b. It is obvious that under conditions such as the foregoing, the laws of probability are bound to operate to produce inadvertent leakage of information, even though the question of loyalty may not enter into the picture at all. The chance for loss of documents increases *in direct proportion* certainly with the number of documents disseminated, and in the COMINT field the loss of a single document, sometimes regardless of its specific contents, may have disastrous consequences - if the document should fall into the wrong hands it will most certainly be followed by such consequences upon our COMINT activities.

10. During World War II certain special security safeguards were established in particular segments of the German COMINT problem. Actual experience with those safeguards amply demonstrated their feasibility and the practicability of operating successfully with the absolute minimum of dissemination and of maintaining the utmost security under difficult circumstances. That experience constitutes a contradiction of the frequently-heard contention that operational effectiveness of COMINT is inevitably defeated by too strict limitation of dissemination. ^{to consumers}

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

11. It is possible to safeguard COMINT by employing special disguises which will not handicap its usefulness and which at the same time will serve to hide the exact source from which it comes.

12. The latter possibility, together with more rigid limitations on dissemination may be necessary to insure us against the drying up of the sources of this vital information.

~~TOP SECRET ACORN~~