

~~TOP SECRET~~
Office Memorandum • UNITED STATES GOVERNMENT

TO : AFSA-00A; OGB; OOC; OOT, 11; 12
FROM : AFSA-00B
SUBJECT:

DATE 14 December 1950

As per DIRAFSA, please edit and return to DIRAFSA with comment(s) --
prior to 1600, Friday, 15 December 1950.

Respectfully,

Block
R. F. BLOCK,
LTJG, USN

~~TOP SECRET~~

~~TOP SECRET~~ ~~ACORN~~REPORT BY THE USCIB COORDINATOR TO
~~THE UNITED STATES COMMUNICATIONS~~ BOARD INTELLIGENCE

on

MEASURES FOR INCREASED SECURITY OF COMMUNICATION INTELLIGENCE

THE PROBLEM

1. What additional measures should be taken to protect (1) present COMINT sources and (2) such new sources as may be expected soon to yield vital information?

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 the security of present COMINT sources is warranted in the light of the present situation wherein there appears to be a gradual lessening of security in the fact of a more pressing need therefor.

b. The possibility of some approach, in the not distant future, 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.

c. In connection with all 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.

~~TOP SECRET~~ ~~ACORN~~

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 study based upon 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~~

ENCLOSURE

EO 3.3(h)(2)
PL 86-36/50 USC 3605FACTS BEARING UPON THE PROBLEM AND DISCUSSION

1. 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, making the production of COMINT a problem of constantly increasing difficulties. This is true especially as regards COMINT dealing with the []

2. In the face of the increasing difficulties in its production, the demand for COMINT has become even greater and the need for the protection of all COMINT sources increasingly imperative. Not only is this true as regards all current COMINT sources, but we must anticipate even greater needs for the protection of new sources. For example, when as a result of concentrated effort AFSA succeeded in solving certain [] cryptosystems, the fruits thereof were soon denied us because of the withdrawal from usage of all [] high-level systems soon after success in their solution was attained, and 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.

3. a. The basic essentials for effective security control of COMINT have finally been established after years of effort and the security situation has been considerably improved.

b. There is a general appreciation of the value of COMINT and the need for protecting its sources; and we now have the following mechanisms for better protection:

~~TOP SECRET~~ 1~~ACORN~~

~~TOP SECRET ACORN~~

- (1) A federal protective law (Public Law No. 513)
- (2) Improved investigative machinery
- (3) An interdepartmental authority (USCIB)
- (4) A single U.S. producer of high-level COMINT (AFSA)
- (5) Common security standards
- (6) Security agreements with our foreign collaborators

4. a. The part played by USCIB in the foregoing improvements in security ^{is} ~~are~~ notable. USCIB Directive No. 1, approved on 16 November 1948, and revised as of 13 October 1950, provides:

"4. ... The Board will perform such functions as may be required to accomplish its objective, but it will place particular emphasis upon the following:

* * *

(c) Prescribing basic security standards and dissemination policies to protect all Communications Intelligence activities and sources."

b. The same reference (Par. 12) establishes, among other standing committees, a Committee on Security with the following responsibilities:

"(b) Security. Formulation of interdepartmental security and dissemination policies, and coordination of other security matters under cognizance of USCIB."

~~TOP SECRET ACORN~~ 2

~~TOP SECRET ACORN~~

c. USCIB Directive No. 4, approved on 14 January 1949, and revised as of 25 October 1950, establishes "Instructions for the Compartmentation of COMINT information", including certain "Precautions in dissemination and utilization of results."

5. As a consequence of 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.

6. a. Nevertheless, the USCIB Coordinator 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 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.

b. Despite the mechanisms and factors for better control, it is not believed that the security situation has been improved to a degree which warrants brushing aside of all fear that current and future success on high-level problems may be nullified by leakage of information to the Governments whose communications are now being or soon will be successfully attacked. In fact, the basis for continued apprehensions on this score remains the same or even stronger than before, because of certain new factors in the COMINT security picture. Among them are the following:

(1) There has been a steady and substantial increase of both workers and consumers. The list of indoctrinated consumers alone has risen from 594 in February 1947 to 1,332 in June 1950. In addition,

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

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

(2) 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.

(3) 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.)

(4) The dissemination of results is far 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.)

See
TICOM
11/50

(5) There is no over-all authority to insure observance of COMINT security regulations within offices of COMINT consumer agencies and organizations. 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. Inspection

~~TOP SECRET ACORN~~

~~TOP SECRET ACORN~~

authority such as that which was vested in and exercised by the Cryptographic Security Board might well be vested in and exercised by USCIB.)

7. It is obvious that under the foregoing conditions 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 chances for the leakage increases in direct proportion to the number of persons who are taken into the picture; the chances for loss of documents increases in direct proportion to 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 most certainly will be followed by such consequences upon our COMINT activities.

8. 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 an extremely limited number of operational personnel who had a real "need-to-know" and with the absolute minimum of dissemination. That experience proved the possibility of maintaining the utmost security under difficult circumstances and constitutes a contradiction of the frequently-heard contention that operational effectiveness of COMINT is inevitably defeated by too strict limitation of dissemination to consumers.

9. 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.

~~TOP SECRET ACORN~~

~~TOP SECRET~~ ~~ACORN~~

10. 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.

11. a. In considering what additional steps should be taken as soon as possible it is convenient to divide the whole problem of COMINT security into four principal segments:

(1) Security precautions applicable to all steps in the production of the information.

(2) Format of the final product (whether or not the source of the information, when it leaves the production agency, is obvious).

(3) Control of production of copies and their dissemination to consumers.

(4) Security precautions applicable to the operational use of COMINT.

b. Under its charter USCIB prescribes basic security standards and dissemination policies and therefore it has cognizance of all four of the above-mentioned segments.

12. a. The USCIB Coordinator has ^{operational} jurisdiction over only the first segment (Par. 11a(1)) and has instituted within AFSA as rigid security controls in the production of COMINT information as practicable under the mechanics of processing. Compartmentation has been especially rigid in respect to the processing of the principal high-level cryptosystems and it is doubtful whether further steps can be taken in that direction

~~TOP SECRET~~ ⁶ ~~ACORN~~

~~TOP SECRET ACORN~~

toward increased security. However, USCIB may wish to look into this question and inquiry is welcomed by DIRAFSA.

b. The USCIB Coordinator has no jurisdiction, however, over the other three segments of the problem and believes that it is to those areas, especially (2) and (3), that USCIB should now direct its attention.

c. The USCIB Security Committee could be directed to study those segments of the problem and submit recommendations as regards the greater security protection of current as well as anticipated new sources of COMINT.

~~TOP SECRET ACORN~~