

~~TOP SECRET~~

22

~~TOP SECRET~~

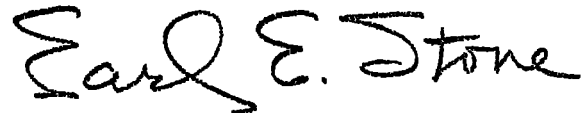
USCIB: 13/134

22 December 1950

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Measures for Increased Security of Communication
Intelligence (COMINT).

1. I have had the attached study prepared in AFSA, and present it for your consideration, with a view to discussing the problem at the next meeting of USCIB.
2. The Coordinator, for reasons set forth in the attached report, is becoming increasingly concerned over what appears to be a gradual weakening of the security of COMINT.



EARL E. STONE
Rear Admiral, U.S. Navy
Director, Armed Forces Security Agency
USCIB Coordinator

USCIB: 13/134

Declassified and approved for release by NSA on 05-22-2014 pursuant to E.O. 13526

~~TOP SECRET~~

REPORT BY THE USCIB COORDINATOR

to the

UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD (USCIB)

on

MEASURES FOR INCREASED SECURITY OF COMMUNICATION INTELLIGENCE (COMINT)

THE PROBLEM

1. To determine what additional measures should be taken to protect present and future COMINT sources.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure herewith.

CONCLUSIONS

3. It is concluded that:

a. A review of all phases of COMINT security is warranted by the present need for increased protection of all COMINT sources and by the evident increases in hazards to COMINT security.

b. It is essential to determine whether any additional measures should be established to prevent a repetition of recent losses, which may well have been due to leaks.

c. It may be advisable, for the protection of high-level COMINT sources, to institute particularly stringent security safeguards such as those in force in connection with certain high-level COMINT problems in World War II.

RECOMMENDATIONS

4. It is recommended that the United States Communications Intelligence Board:

a. Approve the above conclusions.

b. Direct the USCIB Security Committee to make the review referred to in paragraph 3a. and to include in their report specific recommendations pertinent to paragraphs 3b. and 3c.

c. Direct the USCIB Security Committee to submit its report to USCIB not later than 1 February 1951.

ENCLOSURE

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. Since the end of World War II there has been a considerable improvement in the security of crypto systems employed by foreign governments, and a rather general tightening of communication security practices, making the production of COMINT increasingly difficult.

2. Concurrently, there has been a demand for more COMINT and for wider dissemination of it. The need for the protection of COMINT sources is therefore increasingly important. This need must be considered not only from the standpoint of current sources, but in the light of COMINT potentialities as well.

3. The essential features of effective security control of COMINT have been established gradually during years of effort, and the security foundation is considered to be sound. There is adequate appreciation of the value of COMINT, and of the need for protecting its sources. There is, however, no ground for complacency concerning the current state of security effectiveness, in practice. USCIB has played an important role in development of current COMINT security policies and doctrines, and can be expected to play an equally important one in the perfecting of their implementation and observance.

4. We now have the following mechanisms for protection:

- a. An interdepartmental authority (USCIB).
- b. A Federal protective law (Public Law No. 513).
- c. Improved investigative machinery.
- d. Common security standards among U.S. agencies concerned with COMINT.
- e. Security agreements with authorized foreign collaborators.
- f. A single U.S. producer of high-level COMINT (AFSA).

Some of these mechanisms are not yet complete. For example, the existence of Public Law No. 513 should be made known to publishers, reporters, etc.; and there should be a speed-up in investigative procedures to permit more rapid clearance of personnel, with no sacrifice of thoroughness.

5. Although important and basic steps have been taken since the war to establish security on a firm foundation, certain developments have, to a considerable extent, nullified the effects of our advances by introducing additional hazards. Despite the existing mechanisms for control, it is believed that present security is not adequate to insure against fatal leakage of information of our success in the solution of high-level problems. The basis of the Coordinator's continued apprehension on this score is strengthened by certain new factors in the field of COMINT. Among them are the following:

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

b. Certain dissemination safeguards have gradually been relaxed. Material is now distributed to and maintained in a number of areas in Washington, outside the producing agencies, where it was never permitted before. Moreover, distribution to personnel of additional agencies, e.g., AEC, ECA, NSRB, RDB, and probably others, has been authorized. In addition, restrictions on the distribution of COMINT material to, and its retention in, overseas occupied areas have been eased.

c. The administrative, control, and budgetary machinery and procedures are such that large numbers of individuals must now be apprised of numerous details of COMINT activities. (The multiplicity of agencies, offices, boards, and committees concerned with the operation and administration of COMINT activities necessitates distribution beyond COMINT agencies of innumerable reports, justifications, etc., which, in the aggregate, are hazardous to security.)

d. The dissemination of results is far too voluminous for safety. (It is estimated that about 750,000 copies of COMINT translations, representing some 16,000 individual decrypted messages, were distributed in September, 1950, to consumer agencies.)

~~TOP SECRET~~

e. There is no over-all authority to insure observance of COMINT security regulations within the COMINT consumer agencies and organizations. Possibly too much individual authority and discretion in the application of the common principles are left to individual consumer and producer agencies. (The security control of atomic energy information is an example of more centralized and rigid control.)

f. Not only has there been a significant increase in the number of persons who have been brought into the COMINT sphere since the end of hostilities in 1945, but also there has been an increase in the rate of replacement and turnover. In time of war, because of rotation of personnel to overseas units, this turnover rate may be expected to become greater.

g. Since the end of hostilities in 1945, and especially since the recent outbreak of new overt hostilities, the presence of indoctrinated personnel (particularly ground and air personnel) in combat areas has increased the danger of compromise of COMINT information through capture.

h. The probability of imminent military and political collaboration with allied nations other than the British (NATO) will pose additional and more difficult problems in the field of COMINT security, especially if collaboration should include dissemination and usage of COMINT material.

6. It is obvious that under these conditions the laws of probability are bound to operate against the continued security of COMINT. The chances of inadvertent leakage of information, even aside from all considerations of loyalty, increase as the area of dissemination of COMINT increases, since these chances increase in direct proportion to the number of persons who know the secrets, and the chances of inadvertent loss of documents increase in direct proportion to the number of documents disseminated. In precisely the same way, the chances of a foreign enemy agent's success in covert operations to acquire COMINT information increase as the number of his targets increases. In the COMINT field, the loss of a single document, sometimes regardless of its specific contents, may have disastrous consequences.

7. During World War II certain special security safeguards were established in particular segments of the high-level German COMINT problem. Actual experience with those safeguards amply demonstrated their feasibility and the practicability of operating successfully with an extremely limited number of operating personnel who had a real "need-to-know", and with the absolute minimum of dissemination. That experience proved the practicability of maintaining the utmost security of high-level material under difficult circumstances without any detriment to military operational effectiveness.

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

9. In the consideration of what additional steps should be taken, it is convenient to divide the whole problem of COMINT security into four principal segments:

- a. Security precautions applicable to all steps in the production of information.
- b. Format of final products (in its relation to revelation of source).
- c. Accounting control of production of copies, and of their dissemination to consumers.
- d. Security precautions applicable to the operational use of COMINT.
(Including maximum extent to which COMINT can be safely downgraded for tactical use by cover echelons)

Under its charter USCIB prescribes basic security standards and dissemination policies and therefore has cognizance over all of these aspects.

10. The USCIB Coordinator (in his capacity as Director, AFSA) has full operational jurisdiction over the first of these (paragraph 9a.), and has instituted within AFSA as rigid security controls in the production of COMINT information as practicable. Compartmentation has been especially rigid in the processing of the principal high-level crypto-systems, and it is doubtful

that further steps could be taken in that direction without detriment to effectiveness. The USCIB Coordinator has no jurisdiction, however, over the other three segments of the problem and believes that it is to b. and c. that USCIB should direct its attention. The USCIB Security Committee should be directed to study these segments of the problem and to submit appropriate recommendations. The fourth aspect (paragraph 9d.) is primarily a matter under the immediate cognizance of each of the six COMINT consumer agencies.