REF ID: A5197 40

MEMO ROUTING SLIP	NEVER USE FOR APPROV DISAPPROVALS, CONCURRENCES, OR SIMI R ACTIONS.		
1 NAME OR TITLE V. A. Friedman	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE
REMARKS Comment?			
FROM NAME OR TITLE [illegible]		DATE 3 Jan	
ORGANIZATION AND LOCATION AFSA-15		TELEPHONE	

Declassified and approved for release by NSA on 02-06-2014 pursuant to E.O. 13526

DD FORM 1 FEB 50 94 REPLACES NME FORM 94, 1 FEB 49, WHICH MAY BE USED. 16—56363-2 GPO ☆

SEP 2 1952

MEMORANDUM FOR THE CHIEF OF STAFF

SUBJECT: Compromise of Codewords

1. On a Memo Routing Slip dated 20 August 1952, you asked the following questions: "Does COMSEC evaluate codeword violations? If not, who does?"

2. The reply to these questions is as follows:

> The Office of Communication Security evaluates cryptographic or transmission-security compromises of COMINT codewords, reporting to the USCIB Coordinator. Other types of codeword compromises are not evaluated by the Office of Communication Security. In all cases, the USCIB Coordinator has final determination of whether the reported compromise justifies supersession of the existing codeword.

3. The number of reported codeword compromises is indeed alarming. A number of recent actions have been designed to improve the situation.

a. USCIB Directive No. 6 has been revised to provide for more rapid reporting of codeword compromises.

b. USCIB Directive No. 9 has been approved in an effort to provide added protection for COMINT information (the protection of which is more important than the protection of the COMINT codeword).

c. AFSAG 1210 is being reissued to strengthen procedures for reporting of cryptographic or transmission compromises of codewords.

d. The Office of Communication Security has prepared a letter to the Service cryptologic agencies designed to set forth in a body some broad principles of COMSEC for application to COMINT communications.

4. As indicated in paragraph 3.b. above, a realistic approach to the problem of COMINT security would be to do everything possible to insure the security of COMINT information. This does not necesarily extend to the protection of the codeword per se.

5. In many cases of reported codeword "compromise," nothing has been compromised except the codeword in isolation; in some cases, the meaning or use of the word would not be derivable even by inference.

SEP 2 1952

SUBJECT: Compromise of Codewords

---

6. For some time, it has appeared to some people around AFSA that we have had a case of the tail wagging the dog in the relationship of the codeword to the material it is supposed to protect. Much thought has therefore been given from time to time to developing a means of making the codeword the servant rather than the master. One of the results, as you may recall, was the recent recommendation by this Division that codewords be retained for a fixed period of time, regardless of codeword "compromises" which would inevitably occur during that time. The USCIB Coordinator at first agreed, in principle, with this recommendation, but suggested a review of the subject to determine ".... the best unchanging procedure which might or might not be a codeword." On 1 August, a reply to this suggestion was prepared, stating that consideration had been given to the use of symbols, color codes, phrases, and other possible replacements for codewords, but that no satisfactory replacement was found. However, your discussion with Admiral Wenger revealed that the Admiral felt "... we should not loosen up our security any further," and that if the reason for dropping changes in codewords is to solve the printing problem, that can be solved by other means.

7. The recommendation concerning the retention of codewords for a fixed time was not intended primarily to effect savings at the expense of security. Rather, it was a recognition of the fact that codewords have been continued in use for some time after they have been "compromised", without any apparent compromise of the materials designated by the codeword. The Chiefs of the Offices of Communication Security and Operations concurred in this recommendation, but because Admiral Wenger's views on possible security risks are respected, the proposal has been withdrawn.

TRAVIS M. HETHERINGTON
Colonel, USAF
Chief, Plans and Policy Division

REF ID:A59740 TS 52-0489 CR

MEMO ROUTING SLIP

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

1 NAME OR TITLE Chief P+P	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

I am becoming very much alarmed over the increasing number of code-word violations. Some drastic action is indicated if this situation continues. Does ComSec evaluate code-word violations? If not, who does?

EDITION ... [illegible]

... 51 10 22

FROM NAME OR TITLE WFF	DATE 1952
ORGANIZATION AND LOCATION	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used. 16—48487-4 GPO