REF ID:A57049

MEMO ROUTING SLIP

FOR USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE: Mr Friedman	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION: S/Sec'y.	DATE		COORDINATION
2		✓	FILE
		✓	INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

SECRET

MATERIAL ATTACH

REMARKS

As a result of our recent discussion on the number and type of violations & compromises and violations in the monthly reports, I had it prepare the attached comments. I believe they will answer some of the questions you had in mind and forecast an improvement in future reports.

FROM NAME OR TITLE: [illegible]	DATE: 6 JAN 51
ORGANIZATION AND LOCATION: DD/ Comsec	TELEPHONE

DD FORM 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ 16—48487-4 GPO

~~SECRET~~

DD/COMSEC 21 Dec 54

NSA-41

Briefing

1. The following comments are furnished per your request for a briefing on the situation with regard to certain types of violations as noted in the monthly report. I shall be glad to discuss further with you if you so desire.

2. In February 1954, USCIB Directive No. 9 on COMINT compromise reporting procedure became effective. Since then, there has been a steady increase in such reports. In August, further detailed reporting instructions were issued to the Service Cryptologic Agencies in NSA Circular 90-1 (see subparagraph 3e below). The present large volume of compromise reports is not, therefore, necessarily indicative of an actual increase in occurrences; it is possibly due to the dissemination of specific reporting requirements. In either case, the violation volume is high, particularly that of inadvertent clear text transmissions and the encryption of messages in monoalphabetic substitution cipher in on-line operation.

3. Various corrective actions have been taken and recommended, and equipment modifications have been designed to reduce these violations. The status of implementation of these remedies is as follows:

a. A push-button modification for the model 19 teletypewriter and the 131B2 subscriber set has been designed to prevent inadvertent plain text transmissions from the plain text transmitter distributor. The Army has reported installation of this modification on all but a few COMINT terminals. Navy installation is complete. The Air Force has reported installation on the majority of their terminals, and others are being modified as rapidly as modification kits become available. Many of the model 19 teletypewriters used by the Air Force are the commercial type (which has no tape-out button), and special modification kits are required.

b. Another required modification on PYTHON COMINT circuits is the torn tape stop mechanism, which will interrupt transmission within 3 to 15 characters whenever a tape hangs up or runs out. The Army, on 16 Dec, reported installation complete on the ASA Two Rock Ranch terminal and nine (9) terminals in Europe; action has been taken to procure additional modification kits. The Navy no longer has a requirement for this modification, since they have no PYTHON COMINT circuits at present. The Air Force, on 1 Dec, reported that they had on hand a sufficient quantity of TTSMs, and that shipment was being made to command issuing offices for eventual installation on PYTHON COMINT circuits. They will advise us when installations are complete.

~~SECRET~~

c. Instructions have been prepared for the installation of push-button modifications to the SSM-3 and SSM-4 (TT-160/FG, SAMSON) equipments. These instructions will be published in a change to AFSAG 1262-1, which is held by all COMINT field units. Included also in this change will be detailed installation instructions for the torn tape stop mechanism.

d. Serious consideration is being given to installing (or relocating) warning lights to aid in preventing inadvertent plain text transmissions from teletypewriter keyboards.

e. The COMINT compromise reporting instructions of NSA Circular 90-1 are in the hands of each COMINT field unit. Violators are required not only to submit a written report of the facts in each case, but must also include a brief description of the training program for COMSEC as applied to COMINT material.

f. A check-off list or questionnaire covering general, cryptographic and transmission security, and the physical security of cryptographic material, has been prepared for issue to each COMINT field unit. This questionnaire, which will provide us with detailed information concerning each COMINT field unit, is to be filled out by the Commanding Officer or Officer in charge in the course of an inspection of his installation, and returned to us with a copy to the Head of the Service Cryptologic Agency concerned. The check list, in draft form, has been submitted to the three Service Cryptologic Agencies for informal review and comment prior to publication.

4. During 1951, 1952 and 1953, our actions in improving the communications security of COMINT were confined largely to recommendations for corrective action and equipment modifications, and requests that the Service Cryptologic Agencies adopt them. In many cases, they were not adopted. Currently, our approach is more realistic, and we have laid very specific and unequivocal requirements on the Services, and have directed compliance. More and more information and guidance material is being distributed at the Service level at which it will do the most good - the field units. The Service Cryptologic Agencies are cooperating fully in implementing our directives and instructions.

5. Equipment failures and mechanical defects are responsible for some violations, but the majority are due to personal error of some kind on the part of the operator. Furthermore, the majority of personnel errors occur at locations where the equipments have not been modified. Universal installation of the equipment modifications described in paragraph 3 above, however, should be completed in the near future, and a direct result should be a reduction in these errors. The modifications are designed to eliminate much of the personal factor in equipment operation.

6. Of course, in the absence of fully automatic equipment, the possibility of human error remains. Equipment modifications are no substitute for care and attention on the part of the operator. The questionnaire (paragraph 3f above)

~~SECRET~~

~~SECRET~~

places great emphasis on command responsibility for thorough indoctrination and training of cryptographers, and will unquestionably result in a more intensive training program in each COMINT field unit.

7. Actually, we are in a transition period. Definite goals have been established, and the means of attaining them provided. Full employment of these means has taken time, but much progress has been made. The present outlook for the communications security of our COMINT is an optimistic one.

F. C. AUSTIN
Chief, NSA-41

~~SECRET~~