MEMO ROUTING SLIP

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

1 NAME OR TITLE: Col. Sears	INITIALS: KCS		CIRCULATE
ORGANIZATION AND LOCATION: AFSA-04	DATE		COORDINATION
2 AFSA-04			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Re Survey of undertook on Security of AFSA Communication Circuits:

1) Has survey been completed?
2) If so, may I see a copy?

AFJ Send them one if you have one

FROM NAME OR TITLE: AFJ

ORGANIZATION AND LOCATION: DOT

DATE: 6 Aug 57

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.

GPO 1951 - O 975584

TOP SECRET

25 April 1951

Extra cy

411C
for Retention

SUMMARY REPORT ON SECURITY OF AFSA COMMUNICATIONS

D/F to OOB dtgmail 27 Apr 51

I. INTRODUCTION

1. AFSA-04 has been engaged over the last several months in an analysis of AFSA communications for the purpose of determining the types and extensiveness of information potentially available to foreign traffic analysis through similar studies. Voluminous amounts of detailed technical data have been compiled, and consolidation of the material into a final complete report has proven so time-consuming that a summary report of findings is considered essential and is contained herein. The detailed report, when completed, will serve chiefly as reference material for future studies. The study is based primarily on analysis performed on all messages handled between the AFSA processing center and intercept activities during the period 15 June - 15 July, 1950. (A volume breakdown by originating station during the base period of study is attached as Inclosure 1.) Inasmuch as AFSA communication procedures have remained basically unchanged, findings based on traffic of that period are generally true of the situation at present. The report also incorporates results of subsequent spot checks on the same traffic, and results of continuous review of traffic handled at the ARS and NSS communications centers.

II. SUMMARY OF CHARACTERISTICS OF INTERCEPT TRAFFIC

2. The communications of AFSA would gain the attention of foreign traffic analysts in the course of elementary studies of U. S. military

TOP SECRET

TOP SECRET

communications. Such studies would entail segregation of encrypted traffic by external characteristics. It would be noted that a distinctive general system, characterized by an eight letter message indicator, contains the vast bulk of all encrypted traffic of the Armed Forces, and that well over 90% of the traffic in this system is routed to UEPSS, which can be identified as Arlington Hall Station. The originators of this traffic are designated on each message by means of fixed address groups. These same originators send and receive messages in other general systems with routing to UEPAS or NSFN. A number of characteristics inherent in R/I activity are evident in AFSA communications. Among these are:

(a) The worldwide nature of the organization can be determined easily by cryptonet reconstruction.

(b) The volume of traffic in the cryptonet is extremely heavy (60-85% of all Armed Forces encrypted traffic).

(c) Practically all of the traffic is routed to or from one central location, identifiable as Arlington Hall Station.

(d) Traffic flow is almost entirely unidirectional (99% into Arlington).

(e) Technical nature of the traffic is indicated by non-conformance to command channels as opposed to normal command, administrative or operational traffic.

(f) Large volumes originate from locations which are apparently not of adequate military significance to warrant such volume.

TOP SECRET

(g) Occasional plain-language disclosures occur which contain phrases such as "raw traffic," or even unencrypted intercepts.

3. Analysis of data leading to establishment of these characteristics inevitably results in conclusions that AFSA intercept traffic can be identified as such. These conclusions are substantiated by easily accessible collateral information. Specific operating practices which either provide additional substantiating evidence or are potential sources of further insecurity are separately considered below.

a. Control serial numbers. The practice, peculiar to intercept traffic, of using a special set of serial numbers externally to aid in maintaining continuity of traffic flow, is considered to provide enemy intercept with a definite aid in checking continuity of his intercept, or if he so desires, a means of checking our intercept volume with a minimum of effort.

b. Variable system indicators. Given good intercept coverage and a basic knowledge of intercept operations, there is evidence to indicate that the variable indicator system can be solved and that traffic originated by individual stations may be categorized into the traffic types represented by the variable indicators. When this is accomplished, it is possible to compare one station against another with respect to general intercept control objectives, intercept capabilities of individual stations, etc. With exceptionally good coverage by foreign intercept, such information is used to reveal the significance of traffic totals resulting from events of international importance, thus defining missions more clearly and reflecting U. S. intelligence

requirements. For example, a study of [redacted] totals immediately before and after the invasion of South Korea reveals that that station took the lead in interception of North Korean military circuits. Although U. S. intelligence requirements are obvious in this case, situations may arise in the future involving U. S. intelligence requirements which are less obvious, and could be revealed only through fluctuations in AFSA totals. When the general mission at a given installation is known or suspected, further details, including the specific circuits monitored, might be obtained by manipulation of traffic flow on foreign circuits and observation of effects on raw traffic totals. When details of intercept control have been reconstructed to the point that specific targets are identified, it is conceivable that inferences may be drawn regarding exploitability of foreign traffic.

c. Call signs and addressing information. Ample evidence is present to permit general identification of activities involved, to establish realistic linkages between AFSA, AHS, AFSS and NSS, and to tie in the collection activity with disseminating activities.

d. Precedence. In general, precedences are quite uniform, and become revealing only when unusually high precedence from intercept stations can be linked with significant enemy activity. This has occurred on a number of occasions. (See Inclosure 2.)

e. Reruns. Traffic from intercept stations is also characterized by an unusually high rate of reruns compared to other military traffic. Although no particular intelligence significance is attached to this factor, it serves to improve foreign intercept coverage.

f. Traffic types. Based on categorization of traffic by type, and identification of the types, each type has characteristics of its own. For example, identification of one type as weather results in notation that almost all weather intercepts are obtained at stations in the Pacific area. The assumption follows that this traffic consists of encrypted weather transmissions from Asian stations. Although this analysis project did not include monitoring of inter-communication between intercept stations, it is understood that copies of weather traffic intercepted at Guam (the largest source of such traffic forwarded to AFSA) are forwarded to LUEI [redacted] This may be interpreted as indicating the existence of a processing unit at that location, an assumption supported by a flow of traffic during June from LUEI to Andrews AFB, known to be the headquarters of the Air Force Weather Service.

g. Cryptographic characteristics. A study of the eight-letter indicators used on scrambled text reveals several non-random selections. An occasional pair of messages with identical indicators was found. Identicals in the first and eighth positions of individual indicators occurred at a rate far lower than expected random, suggesting that such occurrences are normally suppressed but appear occasionally as violations of crypto-operating instructions. There was a high rate of repetition of a given letter in the same position of several consecutive indicators. Frequency counts on letters used per position per station per day reveal that stations may be grouped according to distinctive frequency distribution patterns; that within these groupings the patterns for any one of the first six positions vary daily, although a given pattern may

recur in the same position or in any other of the first six positions; that, also within these groupings, the seventh position pattern is the same from day to day. Selection of the eighth letter appeared to be random except for avoidance of letters identical to those used in the first position.

(h) Operator efficiency and discipline. Traffic examined by procedure analysts totalled 25,631 messages. The overall discrepancy average (0.12 per message) compares favorably with the average of all military stations (more than one per message). Immediate corrective action was taken on the more serious violations and practices as exemplified by Inclosures 3 through 8.

III. NON-INTERCEPT COMMUNICATIONS OF AFSA AND RELATED ACTIVITIES.

4. Relationship between AFSA and the service cryptologic agencies having been established through communications associations (see paragraph 3e above), valid assumptions concerning their respective functions are made on the basis of volumes and types of traffic, other communications contacts, plain language messages, and an abundance of unclassified collateral information. The bulk of the non-intercept traffic can be grouped into three major categories on the basis of cryptonets, addressees, length, volume and direction of traffic. One of these deserves immediate consideration in that sufficient evidence is present to indicate that its purpose is the dissemination of COMINT products. Through analysis of volume, precedences, and addressees, cryptonets in this group may well provide foreign analysts with an index to the amount of COMINT success enjoyed by AFSA. For example, a

significant increase in the volume of intercept traffic received from [redacted] subsequent to the invasion of South Korea was accompanied by a considerable increase in traffic from Arlington Hall to CINCFE, both in message volume and length. Precedences rose from routine and priority to operational immediate and emergency. These messages were assumed to contain intelligence derived from North Korean intercept and the high precedences indicated that the traffic was of vital importance to the tactical efforts of the U. N. forces. This is cited by way of example, for a number of other significant and informative patterns were noted in this type of traffic. Incidentally, the matter of precedences was taken up immediately with the originators of the traffic involved with the result that a noticeable lowering of precedence followed. The entire problem of communications involved in dissemination has been discussed at length with security representatives of ASA and Cp-202, and it is hoped that operationally feasible cover plans can be implemented.

IV. PROTECTIVE ACTION.

5. The findings reported above indicate generally that the security of AFSA electrical communications is inadequate. Ideally, protective action would involve the removal of characteristics which permit the segregation of AFSA traffic and the identification of address designations. The removal of these characteristics is an extremely complex transmission security problem since AFSA is faced with the task of restoring protection to an identified organization rather than initially establishing protection for a new organization. A disguise is needed and AFSA can effect this disguise only by either

passing itself off as one or more unrelated organizations presently in existence or as one or more new organizations which challenge identification. In either case, the disappearance of the present form of AFSA communications would coincide with (and may be identified with) the establishment of AFSA communications in the disguised form. The problem, somewhat oversimplified, is one of hiding a large object within a small object, and cannot be resolved unless both objects are joined and all external features of both become identical and are protected. An ideal example of such a solution would be complete on-line encryption on a trunk circuit used by AFSA and a wide variety of other organizations. It is concluded that it is impossible to remove characteristics which permit segregation of AFSA traffic or the identification of AFSA address designations, unless wholesale changes are made in the external characteristics of non-AFSA communications, or unless the volume of AFSA electrical communications is considerably reduced.

6. Wherever possible, AFSA-04 has taken corrective action on individual aspects of the overall problem. Until such time as a practical solution to the entire problem is advanced, AFSA-04 proposes to maintain surveillance and recommend improvements on specific aspects wherever indicated. Comments and recommendations on some of the inherent characteristics which contribute to the complexity of the problem, but are somewhat beyond the scope of AFSA-04, are contained in the remaining paragraphs.

7. It is strongly recommended that the requirements for electrical transmission of intercept data be carefully reviewed by competent personnel OTHER THAN THOSE DIRECTLY ENGAGED IN PRODUCTION ACTIVITIES and that such

Review be on a continuing periodic basis; that procedures be established, accompanied by intensive personnel training, to facilitate recognition of exploitable data in the field; that requirements for transmission by electrical means be made more realistic in terms of exploitability; that the possibility of establishing an exclusively AFSA courier service to handle the volume of data not immediately exploitable be thoroughly investigated. It is believed that a courier service could be organized on a more effective, efficient, reliable and secure basis than is possible under communications conditions existing today.

8. The cryptosystem used for the transmission of raw intercept to Washington is considered barely adequate from the security standpoint. Designated as MINERVA, it is a non-one-time additive key generator, presenting the possibilities of solution of pairs of messages in depth whether or not the rotors are known, and, given the rotors, the possibility of identifying and setting the rotors and switches to permit the reading of traffic in one cryptoperiod if a rotor alignment is transmitted in the clear. It is therefore recommended that the cryptosystem known as APOLLO (one time use of ASAM 2-1), with the one-time pad indicator procedure proposed to AFSA-02 in AFSA-04 D/F dated 26 June 1950, be reconsidered for intercept use, and that it be placed in effect as soon as possible as an interim system pending the availability of the ASAM 9, a cipher relatively immune to depth reading and reconstruction.

9. Any contemplated move of AFSA activities would provide the first real opportunity to overcome inherent weaknesses, particularly overt

association of collection and production activities with disseminating agencies. Communications planning should begin concurrently with any movement plans, and full consideration should be given to transmission security implications.

10. A more secure procedure has been devised for providing external identification of traffic by type, and is ready for discussion. However, it is felt that any external segregation of traffic presents inherent security weaknesses. Accordingly, it is strongly recommended that AFSA-02 and AFSA-13 review the expressed requirement for external segregation and all possible solutions based on revision of in-station handling practices be completely exhausted in preference to continuing the present procedure or instituting a new procedure.

SECRET

TOTAL ENCRYPTED TRAFFIC VOLUME
June 15 - July 15, 1950

To AFSA-21	Station	From AFSA-21
1928	USM-4 (ORER)	2
213	USM-5 (HKHH)	
3839	USM-6 (XUHO) *	5
882	USM-7 (YKLB)	
4639	USM-9 (HKPI)	3
5199	USM-11 (LUNA)	
1739	USM-12 (DADX)	2
8690	USM-13 (DAED)	4
1571	USM-14 (HURX)	
98	USM-15 (CACW)	
48	USM-18 (SABK)	
980	USM-19 (AMLJ)	2
632	USM-20 (CADH)	2
106	USM-26 (FABB)	
3115	USM-30 (PEBC)	
701	USM-31A (XCFT)	
824	USM-32 (TEXC)	4
8851	USA-33 (SATA)	7
1854	USM-36 (YKCI)	2
440	USM-37 (KMIS)	
8752	USA-38 (SABL)	8
8154	USM-39 (LUKI)	1
188	USM-83 (VKMC)	
74	USM-85 (TUFP)	3
263	HQ-ASA PAC (HKGJ)	13
26	HQ-ASA EUR (VUDD)	21
Totals- 40,766		78

*Two serial number ranges ran concurrently on traffic out of XUHO, suggesting two separate originators. 52% of the traffic was in a 001-999 range and 48% was in a 3001-3999 range. It was not possible to associate specific ranges with USM-6 or USM-31 as such.

Enclosure 1

SECRET