FY48

~~TOP SECRET~~ GLINT [redacted] [redacted] 7102051

ARMY SECURITY AGENCY

WASHINGTON, D. C.

SUMMARY ANNUAL REPORT

OF THE

ARMY SECURITY AGENCY

FISCAL YEAR 1948

Prepared under the Direction of

CHIEF, ARMY SECURITY AGENCY

July 1950

GAS-22

Front & Back covers must be counted since Code Word is shown

~~TOP SECRET~~ GLINT

1st FRONT COVER COUNTED AS ONE PAGE - TOTAL 82

1

HISTORICAL NOTE

Although this Summary Annual Report of the Army Security Agency is for the Fiscal Year 1948, it was not possible for it to be written earlier because the reports upon which it is based were not available.

It is a brief summary intended primarily only for the Chief of the Agency, viewing the year's work as a whole and making no attempt to differentiate between the responsibilities and successes of the various divisions, branches, and sections of which the Agency is comprised. This information may be found in the various Annual Reports on file in the Historical Subsection.

Historian, GAS-22
July 1950

TABLE OF CONTENTS

LIST OF EXHIBITS

[redacted]
~~6200392~~
7102051

SUMMARY ANNUAL REPORT OF THE

ARMY SECURITY AGENCY

FISCAL YEAR 1948

CHAPTER I. INTRODUCTORY SUMMARY

A. Mission

Throughout the whole Fiscal Year 1948 the Army Security Agency continued its efforts in the fulfillment of its two-fold mission:

1. The preservation of the security of the systems of communications used by the United States Army.
2. The production of intelligence from the intercepted communications of foreign nations, both hostile and friendly.

As in the preceding year, there was no change in the fundamental mission nor in the general organization internally.

B. Operational Highlights of the Year

As will be discussed in greater detail in succeeding chapters of this Report, the year was marked by steady progress in research and development of improved cryptographic equipments and procedures and by equally constant application of more skilled cryptanalytic techniques in the attack upon foreign systems of communications.

Achievements in communications security[1] during the year

[1] See Chapter II this report.

5

were high lighted by the move to protect certain high-grade cryptographic principles during the tense international situation. A program was iniated to replace the SIGABA (ASAM-1) with the SIGROD (ASAM-5) in areas where the dangers of physical compromise were increasing. Considerable progress had been made by the end of the fiscal year. Of equal importance was a successful attempt to reduce the time required to wire a rotor having soldered interconnections. A new rotor was developed, using circuits which can be "printed" with metallic substances on a non-conducting plastic plate, and it was regarded as possible for three workers to produce a thousand such rotors in a day. The old method required the services of a skilled worker for at least a half hour to produce one rotor.

In addition to these developments, the policy was established to design a base unit that could be used with different cipher components. For example, one base unit was evolved which would fulfill most requirements for teletype encipherment requirements. The concept of a base unit with interchangeable cryptocomponents would also provide low-echelon groups with one set of cryptocomponents for field testing, training, or maneuvers, and another set for use when needed and given special protection prior to issuance. Emphasis was also placed upon decreasing the size and volume of mechanical equipment which resulted in reductions up to 200 and 300 per cent.

Two other achievements in communications security during the year added efficiency and accuracy to the operations of the Agency. The first of these involved a change in the system of nomenclature used for all material peculiar to the Army Security Agency. The old system lacked flexibility and was beginning to cause confusion in the field. Under the new procedure, short titles formerly beginning with SIG (e.g. SIGROD, SIGABA) now begin with ASA (e.g. ASAM-5, ASAM-1). The other accomplishment led to the approval for expansion and development, on 13 April 1948, of the Crypto-Communications Plan (ASAG-22) which provides an official guide for the development, testing, and procurement of crypto-communication mechanisms for the Army and Air Force.

In the production of intelligence,[2] increased attention was given to the communications of Russia and Eastern Europe who were steadily tightening their security measures. To meet the mounting demands for intelligence concerning these areas, increased emphasis was placed with considerable success upon the significance of traffic analysis and the exploitation of plain-text intercepts. The interception of Greek Guerrilla and Chinese Communist communications still remained a major problem. A number of new cryptanalytic machines and devices, represented by such examples as the electronic tape comparator, the alphabetic collator, and the [redacted] aided

[2] See Chapter III this Report.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

cryptanalytic progress.[3]

Supporting services which involved laboratories, highly-complex machinery, and the information service continued as heretofore their invaluable contributions to the solution of many difficult problems.

C. Personnel and Fiscal Problems

Strength of the Agency[4] in officer personnel (including warrant officers) was reduced from 445 to 416, mostly as a result of officers being separated to enlist in Grade I and officers leaving to undergo a competitive tour for appointment in the Regular Army. Authorized strength for officers was also reduced during the year from 622 to 480. Enlisted strength had an authorization which was reduced during the year from 5,768 to 3,603, the actual strength being 2,192 at the beginning and 2,713 at the end of the fiscal year. There was a steady increase in the number of officers and enlisted men in pipeline from 797 to 1340. Civilian strength had an authorization of 2,015 at the beginning of the year which was increased to 2,435, while actual strength was 2,258 at the beginning and 2,410 at the end. Recruitment programs were carried on for both enlisted men and civilians.

[3] See Chapter IV this report.

[4] All of the following personnel figures refer to strength as of 1 Jul 47 (the beginning) and 1 Jul 48 (the ending) of the FY 1948.

Budgetary problems were somewhat less serious than in the preceding year. In the following table the first column represents the original estimates requested of the War Department Budget Officer for Fiscal Year 1948; the second column the balance after reductions by that officer; the third column represents the balance after further reductions by the Director of the Budget; and the fourth the amounts appropriated by Congress:

Personnel	$8,840,774	$7,936,758	$7,089,215	$6,640,961
Procurement	5,018,495	4,492,323	2,889,782	2,756,159
Total	$13,859,269	$12,429,081	$9,978,997	$9,397,120

It will be seen that the amount approved by the War Department Budget Officer was 90 per cent of the estimate, that approved by the Director of the Budget 72 per cent, while Congress appropriated about 68 per cent of the original estimate. For the personnel item, the appropriation was only 75 per cent of the estimate and funds appropriated were adequate to pay 2,170 employees, compared with an actual strength of 2,260 and a manpower ceiling of 2,395. For procurement, the amount appropriated was only 55 per cent of what was asked yet it was thought possible that this amount would be adequate. It was expected that obligations by two of the three divisions would be well under the amount available but that in the case of the third (research and development) there would be an actual deficiency of about $400,000. This deficiency was expected, however, to be covered by funds available from the other two divisions.

In order to avoid a reduction in force of civilian employees, the Chief of Staff was requested to approve an additional $600,000 in order to enable the Agency to reach its certified ceiling of 2,395 employees, and his approval was granted in August 1947.

Monthly review of the budget requirements from August 1947 to March 1948 indicated that the budget as a whole was sufficient to cover requirements. The slow rate of civilian recruitment for the first two months after additional funds were obtained made possible a surplus of personnel funds available for transfer to procurement.

In view of reductions made in the budget for Fiscal Year 1949, however, it was decided in March to expedite procurement during the remainder of the year of equipment originally planned for Fiscal Year 1949, if additional funds could be obtained. Overcommittment for procurement was then made with the understanding that if additional funds could not be obtained, the last purchase and contracts would be held over until July 1948. An attempt to obtain $215,000 from the Signal Corps having failed, the Army Comptroller granted an increase in this amount on 15 June 1948. This grant made possible coverage of all but one of the overcommitted contracts which was held up for only a few days until Fiscal Year 1949.

D. Liaison

During this year the Agency continued as heretofore its collaboration with the corresponding agencies in the Navy which, although they are under the same head, the Chief of Naval Communications, operate as separate offices as regards cryptographic and cryptanalytic activities. These activities are, in fact, in separate physical locations. The reasons impelling this collaboration were basically as follows:

1. The necessity for providing adequate security equipment for intercommunication in Joint operations.

2. The elimination of useless or unfruitful duplication of effort.

3. The possibility that a single piece of equipment may serve the needs of two or more services.

4. The possibility that different but coordinated approaches to the solution of the same problem may yield more valuable results than a single approach, especially if the problem is large or involved.

5. The fact that the relatively small number of commercial firms available for cryptographic research and development makes it imperative to use the services of these contractors in coordination with mutual benefit to all.

For many years the Army had been cooperating with the Navy on numerous cryptological projects, not always, it must be admitted, in perfect harmony but with many instances when the collaboration was whole-hearted and extremely profitable to the Nation, e.g. SIGABA/ECM, into which there is no need to enter here. During the War collaboration had been very extensive, particularly on the cryptanalytic side, and the Joint Committee, ANCICC, These factors and differences, along with others, prevented the establishment of a final agreement. Factors which further complicated the negotiations derived from the long-time dual relationship of this Agency and its fields of interest to both the Director of Intelligence and the Chief Signal Officer, and also from the inter-service rivalry which had been heightened by the movement for the unification of the armed services.

Collaboration with the corresponding agencies of the British and Canadians was also maintained for similar reasons. Here, fortunately, the agreements were kept on a relatively low level and collaboration for the most part was concentrated on the cryptanalytic phase of the work. The result was that this liaison ran with greater smoothness than that with the Navy.

CHAPTER II. COMMUNICATIONS SECURITY

During Fiscal Year 1948 the Army Security Agency continued to carry out its mission of protecting the communications systems of the United States Army from potential cryptanalytic attack by the agencies of foreign governments.

In doing this, cryptosystems suitable for record, voice, and facsimile transmissions had to be planned, designed, produced in quantity, stored, and distributed to the users, together with instructions for use and provisions for maintenance. In addition, accurate accounting had to be kept of all of them. A constant check was made upon the actual security of the systems in use as well as upon the potential security of proposed systems or mechanisms in research and development. Vigilant search for cryptographic and physical compromise was maintained at all times. Above all, the personnel of the Agency had to be constantly alert to the possibility of using new scientific discoveries in the interests of communications security.

Much of this activity was, of course, of a routine nature. The organization in existence at the beginning of the fiscal year had been performing its mission without important changes since the end of the war. Consequently, in a report of this kind, only the more important developments can be touched upon.

On 13 April 1948 the Crypto-Communications Plan (ASAG-22), which had been established at the close of the war under the short title SIGIRA, was approved for expansion and development thereafter. It provides an official guide for the development, testing, and procurement of future crypto-communication mechanisms for the Army and the Air Force. Factors which entered into the preparation of the plan were (1) classes of users, (2) means of communication available to them, (3) fundamental principles which govern crypto-communications in general, (4) the stated requirements of the users, (5) simplicity of operation, (6) fitness for operation under varying condition of weather and climate, and (7) ease of destruction in case of danger.

During this year also a change was made in the system of nomenclature used for all materiel peculiar to the ASA. Heretofore, as a result of the fact that until September 1945 this Agency had been under the command of the Chief Signal Officer, ASA communication-security materiel had been designated with short titles regularly beginning with SIG-, e.g. SIGABA, and so on. Confusion was thereafter likely to exist in field operations if the older terminology were continued. Furthermore, the old method of long and short titles had resulted in a system allowing insufficient adaptability to the handling of complicated equipments. Therefore, at the stimulus of the Chief Signal Officer himself, a new system was devised for gradual introduction. Replacing the trigraph SIG- was the trigraph ASA- to which was added a fourth letter indicating the type of materiel to which the individual item belongs, according to the following table:

M	machine	R	rotor
D	device	G	general cryptographic document
Y	ciphony	B	basic cryptographic document
X	cifax	S	strips
N	intercept	K	key list
F	cryptanalytic	L	pads
P	production	Z	codes
T	tape		

Since the majority of these letters are the initial letter of the name of the type they designate, ease in recognizing the type is expected. In addition, a digit was added to the tetragraph to represent the model or individual item, thus ASAM-1 is the first cipher machine, Converter M-134C, formerly known as SIGABA. The principal items now in use are as follows:

New Titles	Old Titles
ASAM 1	Converter M-134-C (SIGABA)
ASAM 1A	Cipher Unit (SIGIVI)
ASAM 1B	Special Cipher Unit (constituting Combined Cipher Machine) (SIGAMUG)
ASAM 1/1	Crypto-operating Instructions (SIGQZF)
ASAM 1/2	Maintenance Instructions (SIGKKK-2)
ASAM 2	Converter M-228 (SIGCUM)
ASAM 2/1	Crypto-operating Instructions (SIGMES, SIGMIK, SIGMOM, SIGYEG)
ASAM 2/2	Maintenance Instructions (SIGHOBY)
ASAM 3	Converter M-228 (M) (SIGHUAD)
ASAM 3/1	Crypto-operating Instructions (SIGLOP)
ASAM 4	Converter M-294 (SIGNIN)
ASAM 4A	Cipher Unit (SIGROCO)
ASAM 4B	Safe (SIGPRAB)
ASAM 4/1	Crypto-operating Instructions (SIGPOB)
ASAM 4/2	Maintenance Instructions (SIGDOLM)
ASAM 5	Converter MX-783/U (SIGROD)
ASAM 5/1	Crypto-operating Instructions (SIGBEC)
ASAM 5/2	Maintenance Instructions (SIGLIL)
ASAM 7	Converter MX-507 (proposed)
ASAM 12	Converter Attachment AN/CMC 12 (HALF JODO)

ASAT 1/1	Operating Instructions for One-time Tapes (SIGSAP)
ASAS 1/1	Operating Instructions for the Strip Cipher Device (SIGUHR)
ASAG 2	Cryptographic Operations
ASAY 2	Speech Equipment AN/GSQ-2

It will be remembered that in the Annual Report for Fiscal Year 1947, considerable attention was given to the development of the SIGROD (ASAM-5) cipher machine, designed to replace the SIGABA (ASAM-1) in areas where the danger of physical compromise was rapidly becoming much greater. The problem of distributing this new machine to military attaches engaged attention in this year, since the Director of Intelligence had expressed the desire that military attaches have a high grade cipher machine. In view of the general plan to replace SIGABA with SIGROD and the general physical requirements for each, the SIGROD was considered more practical for issuance to military attaches. On the basis of returns of a questionnaire which had been distributed to all military attaches, a study was made of the physical security present at each office where it was planned to install the machine. Distribution was made only when the office was believed to be physically secure enough. Since many of these officers were located at points where it would be difficult for the Army to supply an adequate maintenance service, arrangements were made with the State Department for its maintenance personnel to provide this service.

Distribution of the SIGROD in the SIGABA replacement program was originally planned to be in four phases:

I. A trial period in ASA organizations.

II. Europe and the Atlantic Air Transport Command.

III. The Far East and Airways and Air Communications Service stations of the 59th, 68th, and 71st Groups.

IV. Middle Pacific and Western Hemisphere.

Phase I was completed by 1 August 1947. All units participating reported that the machine had been operating in a highly satisfactory manner and had required only minor maintenance work. Phase II was completed during September 1947.

The problem of Joint communications necessary in the Pacific and the Far East so that Army units could communicate with naval units complicated matters in regard to Phases III and IV of the plan, however. The SIGROD Plan was modified in September 1947 to permit the retention of SIGABA at major headquarters in the Far East Command; Phase IV of the plan was eliminated entirely. This permitted reduction of the construction plans from a thousand SIGROD machines to six hundred. Full-scale production was to stop at 450 machines; construction of the remaining 150 would be carried on by a few workers, with the major portion of personnel placed on the problem of reconditioning SIGABA and SIGCUM machines.[5] By the end of

[5] Unit for unit, it requires slightly longer to recondition a SIGABA or SIGCUM and prepare it for long time storage than to convert a SIGABA to SIGROD.

the fiscal year, 500 SIGROD machines had been constructed at Headquarters, ASA. The Army Security Agency, Pacific, had completed distribution of SIGROD machines and systems in the Pacific area by the end of December 1947. In addition, development of a limited joint SIGROD cryptosystem for the Far East was begun in February 1948 and work commenced on the preparation of rotors and corresponding key lists in an effort to make the system effective 1 July 1948. Meanwhile, SIGABA machines were retained where necessary for joint communications.

Again, it will be remembered that the previous Annual Report discussed the development of the SIGJODO and ASAM 12 (the so-called "Half-JODO") equipments designed to shorten the time needed to convert SIGABA encipherments to a form capable of being transmitted by teletype. In actual operation, however, it turned out that the SIGJODO was even slower than the combination of SIGABA encipherment and SIGCUM transmission, and SIGJODO maintenance was very high. In fact, the SIGJODO required 75 per cent more maintenance time than the SIGABA itself, since its adjustment limits were extremely close. Moreover, the heading had to be punched separately on the tape and it was found that the War Department Signal Center was actually repunching the tape, thus eliminating all of the advantages which SIGJODO was designed to accomplish. It was therefore decided not to issue the SIGJODO to field units at all and to disassemble 23 of the 25 units in existence.[6]

Reports on the operation of the ASAM 12 in the War Department Code Center were much better. No mechanical or electrical difficulties had been found. For this reason, in October 1947 a circuit revision was decided upon which would permit the ASAM 12 to be used for encipherment, something the original model did not permit, as well as decipherment, the only purpose for which it had been designed. In June 1948 four such models were to be service tested, two by the Army, two by the Air Force.

A large group of additional military characteristics for literal cipher equipments was received from the U.S. Air Force, necessitating revision in the philosophy of design of the entire cipher machine program. It became obvious that it was impractical to build a large number of individual equipments for each special requirement, and the policy was therefore established to design a base unit that could be used with various and different cipher components. Specifically, one base unit was evolved which would fulfill most requirements for teletype encipherment equipment and thus satisfy the military characteristics of USAF and Army Field Forces for the ASAM 8, ASAM 9, ASAM 13, and ASAM 15. In addition to the obvious economy in manufacture and development, this type of

[6] This would permit utilization of all components of the device having an original value of $85,002.

construction also has valuable cryptographic advantages. It permits the base unit to be of low security classification with a minimum of physical safeguarding; it permits the development of highly secure cryptocomponents for use in wartime and the peacetime use of cryptocomponents which would not divulge any new and highly secure cryptoprinciples; and it permits the issuance to field units of one base unit with any required number of cryptocomponents to fulfill all of the teletype encipherment requirements. This policy is being extended in an effort to provide similar'advantages to off-line literal equipments.

In connection with these developments, the question of whether or not to utilize high-security cryptographic principles in devices intended for low-echelon distribution has long presented a pair of controversial alternatives. From the point of view of security it was desired that the best principles available be incorporated; but from the point of view of intelligence it was feared that the capture of a device embodying the best-known principles presented a serious risk, if other nations adopted such principles too. A policy in regard to this problem had been established on 6 April 1946.[7] A decision in March 1947 in connection with the development of the Converter MX-519()/U, an interim device to satisfy BMR III and IV as set

[7] See Summary Annual Report, ASA, FY 46, p. 19.

forth in SIGIRA, is of interest in regard to this policy in as much as this decision contributed to communication security in low echelons. As approved by the Deputy Chief, Army Security Agency, 27 March 1947 (Tab 1), it provided that each item of communication security equipment intended for issue to echelons of command below Division Headquarters and corresponding Air Force units will be provided with two types of cryptocomponents: one for use in the equipment when issued for field testing, training or maneuvers; the other for use in the equipment when needed and issued for emergency situations which would be given special protection prior to issue.

With the increased emphasis on a versatile base unit, procedures were evolved for miniaturization in the packaging of mechanical equipments, and for the use of special plastics for all electronic components. Weight and volume savings of 200 to 300 per cent resulted, together with a great improvement in the ease of low-echelon maintenance. The former maintenance difficulties were eliminated, thereby permitting a relatively untrained man to repair a defective equipment by merely ascertaining which main component is faulty, replacing it by a new component, and sending the defective one back to a larger maintenance unit for repair.

Another phase of the miniaturization program was to find whether electronic devices or circuits could be used to replace many of the electro-mechanical or all-mechanical components, so as to eliminate troublesome moving parts. It was determined that wholesale use of electronic circuits would not in itself bring a weight reduction or increase reliability, but that a judicious and skillful marriage of electronic circuits and electro-mechanical elements could result in tremendous improvement in weight and size reduction as well as efficiency. Typical of these improvements was that of power supplies. A single dynamotor was designed to replace the ASAM 9 and individual DC power supplies now weighing about 22 pounds, the result being a reduction to about 6 pounds and one quarter of the volume.

A highly important project concerned the attempt to reduce the time required to wire a rotor having soldered interconnections, this problem having been throughout the war a very serious one. An individual rotor of the type now in use requires the services of one skilled person for at least a half hour. When, as it is anticipated, as many as 5,000 of these rotors may need to be wired in a single day, this problem from the production point of view alone seems to be almost insurmountable. Soon after the story of the "Proximity Fuse" had been released by the War Department and some of the details regarding "printed circuits" became known, representatives of the ASA visited the National Bureau of Standards to acquire further information with a view to determining whether those techniques could be applied to cryptographic rotors. After close study and concentrated effort, a new rotor was developed, using circuits which can readily be "printed" with metallic substances on a non-conducting plastic plate, the printed metallic lines being sufficient to carry the current. As a result, it is anticipated that three persons might produce as many as a thousand such rotors in a single day. A by-product of this development was the cryptographic advantage that might accrue by allowing the users in the field to change the rotor circuits as frequently as once a week, or even to have one set of 10 rotor shells, and a choice from a set of 50 circuit inserts in their daily or weekly set-up. The security advantages are obvious, for a potential enemy attempting to solve traffic thus enciphered would have to consider not only the proper rotor set-up but also the possible permutations of 5 of the 50 rotor inserts.

Development of the Converter ASAM 4 (formerly M-294 or SIGNIN), to replace the large SIGCUM and its associated heavy and bulky 131-set, had progressed during the year to the point where service tests were planned by the Army Field Forces at Fort Bragg and also the USAF. This converter was designed as an integrated tele-crypto-mechanism. That is, it combines the two separate units mentioned above in one unit, it would provide for keyboard or tape teletype signals with security of the same grade as that of the SIGABA.

In the field of ciphony and cifax the development program for the fiscal year likewise consisted of miniaturization, that is, a general reduction in the size, weight, power requirements, and maintenance requirements of all equipments under development. Specific ciphony plans included the USAF service test of Speech Equipment ASAY 2, 3 (AN/GSQ-2,3), modification of Speech Equipment 2, 3 if necessary after engineering and service tests, completion of laboratory work on Speech Equipment ASAY 4 and contractual negotiations for prototype models, further development of major components for Speech Equipment ASAY 5, further design and construction of a laboratory model of Speech Equipment ASAY 6, and further research on pulse-type ciphony systems.[8] The cifax program called for completion of cifax and teletypewriter adapters to be associated with Speech Equipment ASAY 2, 3, completion of keyer components to be incorporated into both ciphony and cifax equipments, construction of a bread-board model and completion of contractual negotiations for an ASAY 2 terminal, and preliminary investigation of television techniques.

The AGF service test of Speech Equipment ASAY 2, 3, was completed in June 1947 and the AAF service test was conducted between July 1947 and September 1947. However, the using forces reported the equipment was not suitable for field use in its present form, and recommended that stability and intelligibility

[8] Speech Equipment ASAY 2, 3, and Speech Equipment ASAY 6 are high echelon ciphony systems. ASAY 4 and ASAY 5 are medium and low-echelon security systems.

be improved and maintenance requirements be decreased. Accordingly, modifications have been undertaken which will improve the reliability of the equipment, eliminate a great portion of key generator maintenance, increase flexibility of the equipment to include teletypewriter and cifax operation, and provide high security.

Two major components to be installed in Speech Equipment ASAY 2, 3, will considerably reduce key generator maintenance. These are the Geared Timing Mechanism and the 1/50 h.p. Synchronous Motor Drive equipment. The problem of providing one-time key for Speech Equipment ASAY 2, 3 was let out on contract. This key medium is considerably smaller in size, less fragile, more easily destroyed when capture is inminent, and has a longer operating period than the one-time key medium of phonograph disks used in Speech Equipment ASAY 1 (SIGSALY). The device was to be available for installation in the early part of the Fiscal Year 1949 and high security was espected.

Similer development was continued on Speech Equipment ASAY 4, ASAY 5, ASAY 6, and considerable general research was undertaken in both ciphony and cifax, limited only by lack of time and personnel.

A study was made of the problem of destruction of cryptographic machines with the view of increasing the degree of destruction by the use of inflammable alloys, wires, and plastics as materials in the construction thereof. Attention was also given to the associated problem of destroying quickly and completely closely-packed printed matter, and of improving the igniter on the M1A1 and M2A1 safe-destroying incendiaries.[9]

A series of interesting tests were made on the winterization of cryptographic equipment. It was found that, if special lubricants are used, the ASAM 1 (SIGABA) operates satisfactorily in temperatures as low as twenty degrees below zero Fahrenheit[10] but not below that; that the ASAM 4 (SIGNIN) operates satisfactorily at 10 degrees above zero, the ASAM 2 (SIGCUM) at 20 degrees below zero; and the one-time tapes (ASAT 1) operate satisfactorily at 30 degrees below zero.

Against the possibility of another war, it was proposed by Security Division that large quantities of certain items of cryptographic materiel be reconditioned and placed in a war reserve, securely protected against moisture and vapor and with metal barriers in the containers. This request was approved by the Acting Deputy Chief, Army Security Agency, during December 1947 and immediate steps were taken to facilitate accomplishment of the project. The materiel to be stored in reserve

[9] Tests and information from the field indicated that the manual and/or electrical detonators could not always be relied upon to ignite the unit. An emergency procedure was instituted by CSGAS-83. Ltr No. 147 dated 9 Jan 48.

[10] This was when special lubricants were used. These same lubricants also permitted satisfactory operation at normal room temperature.

constituted the following:

MATERIEL	NO. OF UNITS
ASAM 1	2,000
ASAM 1A	4,000
ASAM 1B	175
ASAM 2	1,250
ASAM 3	500
ASAM 4	150

The project involving the disposition of the SIGSALY terminals which had been withdrawn from use, mentioned in the previous Annual Report, was completed during this year by the decision to store two terminals which had been in the Pentagon plus an additional one, salvaging the remaining nine of the twelve original terminals.

Further work was done on the very troublesome problem of installing one-time machinery into the Presidential Plane "Independence." The chief difficulty encountered was the problem of getting a satisfactory antenna for transmission and reception. An ASA engineer[11] made several test flights in the plane and recommendations were made for the correction of antennas, but the plane itself was undergoing extensive modifications at Santa Monica, California, and flight tests were no longer possible.

Another continuing project planned for the AFF was the development, in conjunction with the Signal Corps, of the mobile signal center. Seven of these cryptographic vans had

[11] Lt. John A. Smith, SC, Tech Staff, Security Division.

been constructed, the cryptographic part of the work being done by the ASA.

The ASA also cooperated with the project known as Operation SANDSTONE, i.e. the Eniwetok atomic bomb tests in October 1947. The radio traffic of this operation was monitored and traffic-analysis studies were made. Protective procedures were also instituted for the security of the operation.

A study was made to determine the amount of intelligence that might be derived by a potential enemy from the plain-text transmissions of the War Department. The traffic between WAR at Washington and DAAA at Frankfurt, Germany, during the months of January to April 1947 was studied and a report forwarded to the Security Branch, Intelligence Division, WDGS, on the large amount of useful intelligence that can be thus derived by intercepting our present plain-text traffic. While a Special Security Officer was on duty in Moscow from the fall of 1946 to March 1948, special protective measures were taken to conceal the activity of this officer as revealed through traffic. During the year a total of 230,547 violations of transmission security were detected and measures taken to bring these violations to the attention of the persons responsible.

Security studies were made during the year on the ASAM 1 (SIGABA), ASAM 2 (SIGCUM) rotors, ASAM 5 (SIGROD), ASAM 3 (SIGHUAD) indicators, the modification of the now obsolete cipher machine M-209, the Speech Equipment ASAY 2 (AN/GSQ 2), as well as on the possibility of photographic compromise of rotors, a point which was definitely established.[12] A study was made also of the amount of crypto-information which had during the war been divulged to foreign governments, and a plan for inspection of cryptocenters was prepared.

During this year 136 radio reports of suspected cryptographic compromise were received and twelve radio reports of suspected physical compromise. Compromises were declared in five instances, three being cryptographic compromise and two physical compromises. The physical compromises involved the defection of a code clerk in Moscow (Sgt McMillan) and a safe found open in the office of the military attache in Bogota.

The ASA furnished cryptomateriel to other governmental agencies during the year and received payment as follows:

Central Intelligence Agency	$20,655.10
Atomic Energy Commission	4,074.72
Federal Communications Commission	305.50
State Department	37,700.05
Total	$62,735.37

The following table represents the changes made in this year of the cryptonet system:

[12] It was found that 80 per cent of wirings could be recovered from close-up prints. See Annual Report Laboratory Br, FY 48, p. 3.

July 1947		June 1948
CRYPTONET		
15	World-wide	Consists of general and high command SIGABA systems and general and stand-by strip systems.
17	Air and Airways Communications Service World-wide	Revised to replace SIGABA by SIGROD. Consists of one SIGROD and one strip system.
22	European Theater	Revised to replace SIGABA by SIGROD. Consists of general and high command SIGROD systems and a general strip system.
33	Special Security Officer	Replaced by SIGROD system 990
35	Army Security Agency	Replaced by Cryptonet 46.
40	Joint Army-Navy	Revised. Consists of general, high command, and very high command SIGABA, intercept SIGCUM, backup strip and general SIGROD systems.
42	Military Attache	Replaced by Cryptonets 47, 48, and 49.
44	White House	Consists of one SIGABA and one SIGTOT system.
45	Pacific and Far East	Revised to replace SIGABA by SIGROD.[13] Consists of SIGABA, general and high command SIGROD, standby strip and two SIGCUM systems.
46	Army Security Agency	Replaced Cryptonet 35. Consists of general and high command SIGROD and three SIGTOT systems.

[13]. This phase not completed. See page 14 of this report.

July 1947		June 1948
CRYPTONET		
15	World-wide	Consists of general and high command SIGABA systems and general and stand-by strip systems.
17	Air and Airways Communications Service World-wide	Revised to replace SIGABA by SIGROD. Consists of one SIGROD and one strip system.
22	European Theater	Revised to replace SIGABA by SIGROD. Consists of general and high command SIGROD systems and a general strip system.
33	Special Security Officer	Replaced by SIGROD system 990
35	Army Security Agency	Replaced by Cryptonet 46.
40	Joint Army-Navy	Revised. Consists of general, high command, and very high command SIGABA, intercept SIGCUM, backup strip and general SIGROD systems.
42	Military Attache	Replaced by Cryptonets 47, 48, and 49.
44	White House	Consists of one SIGABA and one SIGTOT system.
45	Pacific and Far East	Revised to replace SIGABA by SIGROD.[13] Consists of SIGABA, general and high command SIGROD, standby strip and two SIGCUM systems.
46	Army Security Agency	Replaced Cryptonet 35. Consists of general and high command SIGROD and three SIGTOT systems.

[13] This phase not completed. See page 14 of this report.

		Cryptonets 47, 48, and 49 made effective 1 August 1947 replacing Cryptonet 42 for Military Attaches.
		Cryptonet 50 for use for the Air Force made effective 1 September 1947. Consists of SIGHUAD and SIGTOT systems.
89	Domestic Intelligence	Revised to include additional systems and new number designation.
97	Training	Consists of SIGABA, SIGCUM, SIGWIN, SIGROD, SIGHUAD, M-209, and strip systems.

NON-CRYPTONET SYSTEMS

265	SIGCUM used by AEC	Replaced by SIGTOT 1 Dec 47.
274	SIGCUM for First Army Area	Replaced by SIGTOT 1 Dec 47
462	Strip, Transportation Corps	Continued.
463	Strip, U.S. Troops in IB	Discontinued 1 March 1948.
464	Strip, U.S. Troops in IB	Discontinued 1 March 1948.
		SIGABA system 604 for use by Sandia Base initiated in April 1948.
		SIGHUAD systems 613 and 614 for use between WAR and USAFE initiated in April 1948.
		SIGCUM system 619 for use in the Caribbean initiated in June 1948.
		SIGROD systems 623 and 624 for emergency reserve in London issued in June 1948.

626	State-War-Navy Emergency Strip	Continued. Strip system 815 for emergency reserve in London issued in June 1948. SIGCUM system 875 for Director of Intelligence, Dept of State, Navy. Air Force and Central Intelligence Agency initiated in May 1948.
885	SIGABA for "WORKDAY"[14]	Replaced by SIGROD system 895 and placed in War Reserve status. SIGROD system 890 for ASA and Athens initiated in May 1948. SIGROD system 891 for ASA and Ankara initiated in March 1948. SIGROD system 990 replaced Cryptonet 33 for Special Security Officers on 1 October 1947. SIGHUAD system ASAK 16 thru ASAK 19 for State Department and Central Intelligence Agency initiated in June 1948.

For a time there was a serious problem in the production of sufficient SIGTOT tape. On 7 February 1948 there was a backlog of 33,440 tapes, but additional employees were secured and a swing shift instituted, with the result that the backlog was reduced to 11,000 by the end of the fiscal year.

[14] Short title of Operation MAILBAG changed to WORKDAY during the FY 48 because of a compromise of the MAILBAG code name. The ASA began work on the development of Operation MAILBAG during FY 47.

The following are the production figures for the year:

SIGTOT tapes	89,474
Pages of printed matter	14,845,391
Registered documents printed	121,789
Non-registered documents printed	76,000
Rotors wired	3,317
Machines constructed	746

The following represents the material returned from field:

Registered documents	14,600
Rotors	2,058
Machines	650

The following represents the destruction of cryptographic materiel:

Registered documents	45,901
Non-registered documents	5,004
Rotors	181
Machines (including 36 SIGMYC obsolete)	8,754

Machines and devices shipped to holders totaled as follows:

SIGABA	85
SIGROD	254
SIGCUM	30
SIGHUAD	72
SIGNIN	6
SIGAMUG	168
SIGIVI	145
Miscellaneous rotors	2,423

The packages shipped totaled 17,148 and the pouches 5,023.

CHAPTER III. THE PRODUCTION OF INTELLIGENCE

A. Introduction

In fulfilling its second primary mission, the production of intelligence by means of cryptanalysis and traffic analysis of intercepted communications of foreign governments, both hostile and friendly, the Army Security Agency continued its attack.

During the year, the struggle between East and West was sharply defined. An atmosphere of conflict served as the background for sharp diplomatic exchanges and various political, economic, and military actions and counteractions. The information obtained through the communications-intelligence operation served as a steady and unique source of intelligence as heretofore. With recurring crises in all areas of the world, the pressing demand for pertinent information taxed the capacity of the Army Security Agency and demanded ultimate adaptability in interception, cryptanalysis, and traffic analysis to satisfy shifting priority requirements. For instance, the Greek Guerrilla problem, previously non-existent, became an extremely important and productive problem in 1947, the first translation in this series being published in the latter part of August of that year.

The interception of foreign communications presented several new problems during the year. A progressive change from

Morse-type to radio-printer type transmission necessitated highly-specialized intercept equipment and a large-scale training program for the operators. Interception of Greek Guerrilla and Chinese Communist traffic presented a difficult and complex problem. Cooperation continued as heretofore with the Navy, the British, and the Canadians.

Fiscal Year 1948 also was marked by an intensification of the difficulties facing the Army Security Agency in its efforts to subject the communications of foreign governments, particularly those of the Soviet Union and Eastern Europe, to cryptanalytic attack. Doubtless as a result of wartime experience and growing attention to research and development in cryptological matters, stimulated in all probability by indiscrete disclosures of cryptanalytic successes by this and other governments, the nations of the world have in most instances greatly improved the security of their communications systems. Of no nations is this more true than of the Soviet Government and those central European countries within its orbit.

The dual problem of increased security measures applied by the Russians and their associates coupled with an intensely increased demand for information in regard to these areas, emphasized more strongly than heretofore the significance of traffic analysis and the exploitation of Russian plain text as a source of intelligence. For example, the volume of plain-text intercepts received during 1948 was over 3 times that received during Fiscal Year 1947, and 90 per cent of this total increase was for use in the Russian problem.[15] These intercepts provided a wealth of detailed information on Russian economic and industrial potential. The Russian military traffic-analysis problem and the problems in the satellite areas, particularly Yugoslavia, proved to be almost unique sources of accurate and consistently available information on military organization and activity behind the Iron Curtain.

A continuing difficulty from Fiscal Year 1947 was the particularly acute shortage of highly-qualified linguistic experts of unquestioned loyalty, which necessitated a constant effort to train within the Agency new personnel for competency in various languages. Courses were given during the year in the following: Russian, Greek, Hungarian, Albanian, Serbo-Croatian, French, Italian, Spanish, and Arabic.

The success of the Army Security Agency in accomplishing assigned intelligence missions during the year was officially recognized by the users. The Agency received, for example, a commendation from the Intelligence Division, War Department General Staff, dated 13 August 1947, upon the preparation of DA 13726 and DA 13739. The letter stated that both the Secretary of War and the Director of Intelligence were highly pleased

[15] See page 65 of this report, "Analysis of Production Figures." On 13 Nov 47 a Plain Text Sub-Section was activated in CSGAS-93B to supplant the Pentagon Plain Text Unit which had been organized 17 Apr 47.

with "the rapid, efficient and judicious manner in which these important items of Intelligence information were collected, processed and distributed." From the Acting Special Assistant to the Secretary of State, Mr. W. Park Armstrong, Jr., came a letter addressed to the Director of Intelligence which contained the following significant paragraphs:

> The Department now relies upon the technical facilities and the skills of the Army Security Agency, and the corresponding unit in the Navy, for its basic communication intelligence material, and I should be grateful if you would inform the Chief, ASA, of our appreciation for this indispensable service. It is certainly an outstanding example of interdepartmental collaboration to mutual advantage and in the spirit of teamwork which is now, more than ever, the expressed goal of our government.
>
> The relationship which exists on the working level between our people and yours are still another source of gratification to me, and I shall like to extend our thanks to them through you.

A third gratifying acknowledgement of the usefulness of the ASA's intelligence product came in a letter dated 10 May 1948 signed by the Director of Intelligence, United States Air Force. Major General George C. McDonald referred to a request dated 21 April 1948 for "any available information on Russian air defense organization, operation, and capability, with particular emphasis on air-ground communications." The report promptly forwarded only two days later had proved to be "of great interest and value to this Directorate, not only for information on the subjects requested, but also for the additional information on related items."

During the fiscal year, copies of the Daily Bulletin were regularly supplied to the Intelligence Division, Department of the Army General Staff; to the Navy (CSAW); to the U.S. Air Force; to the State Department; to the Central Intelligence Agency; to the British (LSIC), and the Canadians (CBO). Liaison with the Intelligence Division, D/A GS, was maintained by teletype for use in the case of messages of the highest urgency.

B. Problems of Interception

The efficient interception of foreign communications in accordance with established priorities is, of course, basic to the Army Security Agency's production of intelligence. To fulfill its intercept requirements, the Agency continued to operate its complement of seven fixed monitoring stations, together with five others under Project 78, in an effort to make the coverage as complete as possible according to priorities set up by the Joint Intercept Control Group (JICG). All coded traffic and some plain-text traffic was regularly exchanged with the Navy (CSAW), the British (LSIC), and the Canadians (CBO).

CSAW and ASA continued joint coverage of ICR links under the supervision of the JICG, which also originated the intercept missions performed by CBO stations. The ASA assisted CSAW in the cover of a non-Morse link from a European intercept station (because the ASA had relatively more intercept facilities in Europe) and CSAW devoted several positions in the Pacific to coverage of military and air targets for the benefit of ASA (because CSAW had a more favorable ratio of facilities to Naval targets in the Pacific than existed between ASA facilities and military targets). Comtemplated major changes in intercept assignments were coordinated between ASA (or CSAW) and LSIC (or GBO) in order that a certain degree of informal allocation of coverage responsibility could be maintained.

The progressive conversion of radio links to non-Morse types of transmission was speeded considerably during the fiscal year. On Russian internal links, a total of 9 different non-Morse transmission types were known to be in use: 2-, 3-, 6-, and 9-channel Baudot radio-printer; variable-cycle 3-channel radio-printer; simplex radio-printer; unenciphered radiophone (and, it is believed, scrambled or inverted radiophone); Hellschreiber, and clear facsimile. In addition, several Russian internal links were using, or planning to convert to, a four-tone emission rather than the usual continuous wave or frequency shift keyed emissions. The considerable progress made in providing equipment and personnel for intercept of these transmissions permitted a fair degree of operational exploitation of Russian non-Morse internal links and is expected to permit increased exploitation of all these transmission types during the next fiscal year.

A majority of the ICR links terminating in the U.S. had gone over to radio-printer operation by the end of the fiscal year, and many of the stations using American equipment for communications with U. S. commercial stations were in the process of converting their lateral (i.e. non-U.S. terminal) links to the same type of transmission.

Major problems resulted from the transition period in which assigned intercept missions progressively changed from Morse-type operations to radio-printer type of operations. This change in type of mission made necessary the procurement of highly-specialized types of intercept equipments and the establishment of a large-scale training program for personnel required to operate such equipment. The installation of these specialized types of equipments further resulted in major modifications of the existing intercept stations.

Two additional equipments for intercept of Double Current Cable Code transmissions (used primarily on British Empire circuits) became available during the year, and were put to use in coverage of circuits connecting London, Cairo, Athens, and Berne. Another change during the year involved the conversion of all ASA stations to the procedure of copying on continuous teletype roll paper all transmissions (both traffic and chatter) over manual Morse service links. This project was completed in late November 1947.

During late December 1947 and January 1948, all ASA stations forwarding Russian military and air five-digit intercepts by radio-teletype were instructed to skeletonize this material, i.e., transit by radio only the heading, preamble and first five and last five groups of the text. This was made necessary by the loss of communications personnel at the U. S. Navy intercept station at Adak in the Aleutians, and by the unmanageable increase in the teletype load at ASA. Skeletonizing of five-digit material received from ASA stations was continued throughout the fiscal year, but has since been discontinued.

The trend toward increased use of private links between the foreign offices of various nations and their diplomatic offices abroad continued. At the end of the year, seven nations were operating a total of 119 such circuits. Of this total, 25 were being monitored regularly by ASA facilities and another 41 by facilities of collaborating agencies. The seven countries

[redacted]

Special arrangements were made to obtain coverage of government traffic passed in connection with the Pan-American Conference in Rio during July 1947 and the Foreign Ministers Conference in London during November 1947. Adequate coverage of all other conferences held during the year was possible without disruption of normal missions.

In the Far East, during early 1948 the U. S. Military Attaché in Nanking began obtaining copies of Chinese Communist

EO 3.3(h)(2)
PL 86-36/50 USC 3605

42

radio traffic from an unknown source and delivered this material to ASAPAC for forwarding to this headquarters. Despite intermittent attempts by ASAPAC to intercept CHGB radio links, the military attache in Nanking remained our only source of Chinese Guerrilla traffic throughout the fiscal year. Censorship procurement by Headquarters ASAPAC of all outgoing foreign government traffic from Japan and Korea was initiated on a partial basis during November 1947 and became complete in early April 1948.

In Europe, ECASA during early 1948 began forwarding low-echelon Russian military traffic and T/A reports intercepted and prepared by a group of former German Sigint personnel employed by the ODDI, Eucom.

Highlighting some of the problems met in operating the intercept stations were changes in Signal Corps policies which required reimbursement of funds to the Signal Corps for all Plant Engineering Agency equipment received by ASA. Before Fiscal Year 1948, the Signal Corps had furnished the equipment from existing stocks and did not require reimbursement. During Fiscal Year 1948 the Signal Corps requested that all items peculiar to the ASA be procured, stored, and issued only by the ASA itself. Various items normally considered common to the Army in general were declared peculiar to ASA, which placed an additional work load on the ASA to prepare control levels of spare parts and equipment to be stored here.

Spare parts for all equipment at fixed installations became increasingly difficult to obtain through local supply sources, resulting in emergency procurement of these items by this Agency. These emergency procurements increased by approximately 100 per cent over similar procurements in Fiscal Year 1947.

On the operational level, procurement difficulties existed between ASA and the Signal Corps Procurement Agency in the contracting for items peculiar to ASA. Bids on the equipment were evaluated by Army Security Agency and Signal Corps Laboratories, and in several instances the evaluations given by ASA did not agree with those submitted by Signal Corps Laboratories. Also, procurement through the Signal Corps channels resulted in a time delay of about six months, which in many cases hampered urgent operations.

The current trend of Signal Corps-ASA relationships indicates that the Army Security Agency may become independent of the Signal Corps in the issuance of supplies and equipment required for intercept operations. Budget estimates are now being submitted to cover all material required by the TA units of ASA. This procedure may, in the future, necessitate that ASA set up a supply depot at this headquarters for utilization as a supply source for all ASA fixed-station detachments.

Procedure for the preparation of projects for individual fixed stations has been set up, and it is expected that these projects will ultimately supersede the present station Table of Allowances. It is believed that these projects will ultimately provide a more satisfactory basis for the initial issue of equipment and for the issue of maintenance, supply, and spare parts required for efficient operation of the units.

In order to meet increased demands for intelligence with more thorough coverage of foreign communications circuits, one new intercept station was completed and two others were in the planning stage. The installation of intercept facilities at Herzo Air Base, Germany, was completed during the year. The project and specifications for a new intercept station in the Clark-Stotsenburg area in the Philippines have been completed. In addition, tentative plans of a project for a new station to be located in Okinawa have been compiled and will be forwarded to higher authority for further action in the near future.

C. The Exploitation of Intercepts

The Russian Problem: A general improvement of intercept facilities and personnel made available a steadily rising volume of traffic for processing with a corresponding increase in publication. Though there was a general increase in volume of traffic of all types, the most important single factor in this growth was the 500 per cent increase in Russian plaintext traffic received in Fiscal Year 1948 as compared to Fiscal Year 1947. There was also a 70 per cent increase in code and cipher material over Fiscal Year 1947.[16] The steady expansion of effort on the Russian and satellite countries continued, of course, to be the predominant trend in ASA's production of intelligence. Personnel of the Russian and Bulgarian Section (CSGAS-93-B) increased from 443 in July 1947 to 498 in June 1948 (Tab 2). The complexity of the cryptanalytic problems in these areas, resulting from the adoption and application of more rigid security measures by the Russians and their associates, together with the intense interest in any and all information on these areas, emphasized the potential value of certain aspects of the communications-intelligence operation which had not previously been exploited. The significance of traffic analysis and the exploitation of Russian plain language as a source of intelligence was widely appreciated.

The Russian military traffic analysis problem and the problem in the Russian satellite areas, particularly Yugoslavia, proved to be almost unique sources of accurate and consistently available information on military organization and activity behind the Iron Curtain. For example, through a study of Yugoslav Army field post numbers, a major military move of that army was first noted by the ASA and later confirmed by ground sources. In February 1948 the 27th Division of the Sixth

[16] A total of 1,771,537 messages were processed during FY 48 by the Traffic Processing Unit of the Russian Section.

Yugoslav Army with all its components moved out of the Banja Luka (Bosnia) area south to Ohrid (Macedonia) along the Greek border; division headquarters and all brigades were identified. Addresses placed the headquarters of the division consistently at Banja Luka from December 1946 through February 1948, after which it was noted as addressed at Ohrid. At the same time the brigades, all of which had been addressed at locations in the Banja Luka area for the same period of time, began to be addressed at locations in the Ohrid area along the Greek border. The value of such intelligence to the combat arms is, of course, obvious. The skill and experience of the personnel assigned to the problem had already overcome the complex technical problems involved in deriving the numerous details of Order of Battle date from separate items of traffic. There remained the further problem of assembling the many disconnected pieces of information and reporting them in intelligence form. As a result of thorough investigation and experimentation in this field the various T/A Fusion Reports were developed.

In the field of Russian plain-text, similar problems were encountered and comparable solutions attained. Because of the enormous volume of plain-text intercept made available each month, the translation and publication of each item was obviously a physical impossibility. In addition, such a form of presentation would be of doubtful value and would require a large number of linguists and research analysts at both producing centers and intelligence evaluating agencies.

The wealth of detailed information on Russian economic and industrial potential contained in this body of intercepted traffic made it imperative that the utmost effort be exerted to exploit it fully. This exploitation could be done only if the many separate items on a given subject were carefully studied in the original language and in relation to one another. A synthesis of the information so derived could be put into organized form and then published. As a result the reporting form represented by RUPLAR, RUPLAP, and RUPLAI was developed and supplemented by individual translations of highly significant items.

The development of the plain-text problem emphasized the importance of collateral information in communications intelligence operations. Every effort was made to assist the plain-text analysts with the best available data from other sources on their particular subjects of study, and to supplement these efforts with summaries and reports based on collateral sources.[17]

The Russian [redacted] intercept situation improved slightly during the year, although no appreciable progress was made in the solution of difficulties imposed by geographical factors.

[17] The mission of the Information Section, Information and Documents Branch, CSGAS-95, is to service the staff and operating divisions of ASA with collateral information. See pp.71 &72this report.

PL 86-36/50 USC 3605

For such problems as result from the size of the Soviet Union, its protective wall of satellites, and the geographical location of ASA intercept stations, no satisfactory solution has yet been found. Intercept continues to be concentrated on high-powered main-line nets; cover on secondary and low-echelon nets is possible only in the case of certain favorably-located peripheral areas. In the late spring of 1948 ECASA made an initial effort to intercept low-echelon Soviet military and air networks in Germany. Coverage of high-echelon targets in the European Area continued to increase slightly over the major increase that was noted in the report for 1947.

Nineteen new military Radio Printer links were identified during the year. The presence of these new links is indicative of the general Soviet trend toward increasing use of non-Morse communications facilities. The ASA was able to cope in part with this trend - reflected in military communication by the augmented number of two channel Radio Printer links, and in commercial communications by the increase in single-channel teleprinter - as a result of its non-Morse planning program, which had anticipated such a trend. Although available facilities are not yet adequate completely to handle two-channel links, it is believed that the situation will be appreciably improved by the end of the Fiscal Year 1949. The difficulties impeding effective use of Radio Printer facilities were somewhat alleviated when the stations were supplied with typing reperforators. The stations are now able to see what is being copied, which assists in identification of links; moreover, typing reperforators are invaluable in keeping all equipment in synchronism.

Intercept control was improved and facilitated through the establishment of the system of National Section Intercept Requirements committees, which forward monthly to the Intercept Priorities Allocation Committee requests for coverage. Improvements in the methods of exchange of data with the intercept stations, effective guiding of local T/A groups at the stations themselves, and the special training given to T/A teams to be sent to the stations, resulted in a closer working relationship of ASA with all the intercept stations. At the same time, such a situation resulted in the effective forwarding of T/A data from the stations in daily T/A reports.

Increased concentration was placed (1) on the processing and analysis of search material, and (2) on the careful direction of search assignments at the stations. The result was a more effective search program, which permits the rapid exploitation and development of promising search material.

A noticeable expansion of effort was assigned to Net Analysis. The Soviet Military and Air nets in the Far East, which had been largely reconstructed in 1947, were maintained at their previous level. Such changes as took place were observed and accounted for as they occurred.

Increased effort in the study of European nets, initiated at the end of 1947, was continued in 1948. The result was a complete reconstruction wherever cover was available, which in turn afforded a gratifying flow of intelligence. By the end of the year, the first break into medium-level military and air nets in the European Area had been achieved.

A new air-ground unit, established to study the large air-ground, ground-ground, and ground-air operational nets, originally had concentrated only on the reconstruction of the Far Eastern portion of the nets. As the international situation deteriorated toward the end of the year, however, more and more emphasis had to be placed on the European Area.

Military Baudot analysis was actively continued, and provided a considerable volume of intelligence, as well as a broad base for comparison and cribbing into the more difficult Morse. Nineteen new Radio Printer links (six air and 13 military) were heard and immediately identified as to location and unit served.

Increased effort was placed on the analysis of non-military links, and on illicit, [redacted] a large number of outstations were identified through comparison of

EO 3.3(h)(2)
PL 86-36/50 USC 3605

cryptanalytic elements [redacted]

Existing T/A techniques continued to be refined, new ones developed with reference both to order of battle recovery and to the various signals aspects of traffic analysis (net reconstruction, recovery of enciphered address systems, etc.). New techniques applied to call sign solution and further refinements in techniques for handling Message Serial and Number (NR) data were established.

The cryptanalytic attack upon the Soviet systems was, of course, the most important single intelligence problem facing the ASA during the year. Upon this problem was expended the work of the largest number of skilled technicians, both cryptolinguistic, as well as the activity of a large part of the IBM machines and other supporting techniques such as information gathering and evaluating and the like.

The [redacted] still in the research stage at the end of the previous year, had increased in production rapidly until the system was withdrawn by the Russians in April 1948. Techniques, skills and procedures applied to [redacted] (used by the Far-Eastern Military District and its subordinate corps) had become so highly developed and refined that the almost immediate solution of traffic in this system was commonplace before the system ceased to be found in the traffic in November 1947.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

The loss of both [redacted] was a considerable blow to the productive effort but as a result effort on other Russian projects has been intensified and the projects have been approached with doubled vigor. Intensified effort on operational systems yielded excellent results both from a cryptanalytic and a linguistic point of view, and contributed largely toward building a more complete picture of Russian order of battle.

An ever-growing realization of the necessity for research on key generation in all its phases brought about special emphasis on this aspect of the problem. The coming year will see an intensification of this effort. Techniques devised during the previous year proved efficacious in the solution [redacted] messages,[18] and plans under way anticipated even further success for the following year.

The [redacted] problem became more difficult in May 1948, when the Russians instituted a standardization of format for all three branches of the service: Indicator group and serial numbers are now enciphered [redacted]

[18] [redacted] Little crypto-intelligence is currently obtained since the nature of the system is such that minimum servicing is required.

are now being enciphered by means of the key proper. From a cryptanalytic standpoint, this change will make extremely difficult the finding of new key and the pairing of isomorphs.

Eastern Europe: The Russian influence upon the nations of Eastern Europe[19] which has been consistently observed in their political actions since the War is also reflected in their types of communications systems. As in the case of the systems of the Soviet Government itself, there has here also been a steady increase in security, though as yet these nations have not become so cryptologically mature as their mentors.

Most of the messages intercepted from the Balkan countries [redacted] though there has been some coverage by U. S. monitoring stations. A team for special intercept duty was sent to ECASA with an assignment of intercepting Yugoslav messages which had a very high priority in June 1948 when it became apparent that there might be a break between Tito's government and the Russians. Very good coverage has been received on the "blind" (one-way) link operated from [redacted]

[19] The Balkan and Central European Section (CSGAS-93-D) is responsible for analysis of all non-naval Balkan traffic (except Bulgarian and Romanean) as well as the military traffic of [redacted] countries, and Iceland on which little is done. See Tab 3 for production and personnel chart.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

intercepting the traffic of the Greek guerrilla forces has been exceedingly difficult. These forces do not occupy a very wide territory and consequently their emissions do not need to have high power. As a result, their signals are too weak for interception by U. S. fixed monitoring stations. Special intercept stations, set up for this very purpose, were unable to get close enough for favorable results.[20] Incidentally, this experience may be indicative of the sort of development which a government favorably situated, that is, with a large area of contiguous territory may adopt to prevent radio interception. For example, the Soviet Union with its vast spaces may adopt a system of using a series of low-powered radio stations, each capable of relaying a message for a relatively short distance. Such a procedure might approximate the security of land lines if intercept stations could not reach a favorable position for interception. Net analysis was directed to Yugoslav, Albanian, and Greek (Guerrilla) networks. The Yugoslavian [redacted] Their highly complex air network is fairly well reconstructed, and partial reconstruction of the [redacted] networks have been effected. Reconstruction is complete for the comparatively small Albanian [redacted]

[20] A large volume of Greek Guerilla traffic was intercepted by [redacted] and forwarded to ASA. See pp. of this report.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

and is nearly complete for the police net, but the small volume of intercept has prevented reconstruction of the military network. Reconstruction of the Greek Guerrilla network, a complete and constantly changing net operated by Markos' forces, is virtually complete for stations in continuous existence but much short-lived activity is unidentified. This network, on which work began near the end of Fiscal Year 1947, mushroomed into a major T/A problem involving approximately thirty radio stations which operate in all major areas of Greece except possibly the Peloponnesus. The network also has stations in Bulgaria and Yugoslavia and for some months was tied in with the Russian illicit network. For Czech traffic no work has been done on the illicit network [redacted] Poland's [redacted] net is completely reconstructed, but the [redacted] has resisted solution through lack of sufficient traffic. Partial success has been achieved on the [redacted]

Bulgarian traffic analysis and cryptanalysis was confined [redacted] since the British do the work on the air and police systems of this government. [redacted] [redacted] 1553 were in readable systems, 626 were unreadable, and 1095 were plain-text messages. The police systems produced 5110 intercepts of which 1500 were readable, 1861 unreadable, and 1749 in plain-text. All 155 of the

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

in 1947 2038 unenciphered messages were intercepted as against 27 enciphered, in 1948 these figures were, respectively, 1553 and 626.

In Czech cryptanalysis, work was done in 1948 on nine exploitable systems, compared with only four in 1947. Figures for this traffic for both 1947 and 1948 are given for comparison:

	1947	1948
Cipher Messages	5904	9098
Translations	390	1635
Plain Text Messages	9794	12915
Translations	190	615

[redacted] a simple monoalphabetic substitution system which is completely readable continues to produce the bulk of intelligence. The volume of intercept in this system received from January to June 1948 was 300 per cent greater than in the corresponding period of 1947. The [redacted] polyalphabetic substitution systems [redacted] are, however, the chief systems used by the Czechs and most emphasis was placed on them.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

EO 3.3(h)(2)
PL 86-36/50 USC 3605

The exploitation of police [redacted] traffic of the Czech government, as well as its plain text, contributed greatly in making available accurate information about Czechoslovakia, particularly in the eventful months following the Communist coup in February 1948. During the fiscal year, 53 Czech messages were cited [redacted] as compared with only four in 1947.

Police messages revealed the method of operation of the National Security Organization in Slovakia, Communist penetration into all facets of life - political, educational, religious, and methods used to make the population conform to Communist dogma, as well as means of surveillance, the elimination of dissenters, and rewards for collaborators. [redacted]

[redacted]

Despite difficulties in interception of Greek Guerrilla

EO 3.3(h)(2)
PL 86-36/50 USC 3605

traffic by ASA monitoring stations, voluminous traffic was intercepted [redacted] and this had a high priority in processing. The progress of operations involved constant adjustment in priority assignments on the various single and double transposition systems used by the forces of General Markos, and the transfer and training of linguists. Volume of traffic received rose from an average of 1200 to 3000 messages a month. Guerrilla traffic grew increasingly complex from the early single transpositions received in August 1947 to double transpositions with complex indicator patterns. Five other guerrilla systems in which comparatively little traffic was received became completely readable. This was letter, digit, and mixed traffic, and included polyalphebetic substitution and additive systems. The intelligence derived from the readable Greek guerrilla traffic was the primary source of information on Markos' Army, and included such subjects as order of battle, conscription strength, troop movements, battle reports, supplies, atrocities, civilian population, propaganda activities, and the Greek National Army.

Hungarian [redacted] The problem then was one of production. [redacted] was readable until soon after the Communist coup of May 1947, but two of the three new systems which replaced the older

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

A total of 25,327 Polish messages were received during the year. Of these, [redacted] 5756 internal police and security, 156 military (Frontier Guard), 59 air, and 600 Workers' Party. Cryptanalytic studies were made [redacted] Exploitable systems were chiefly the lower echelon systems of the Internal Security Corps (KBW), one of four Frontier Guard systems, three of the four air systems, and the Workers' Party. [redacted] during the year.

Though the serial numbers of Romanian Foreign Office messages showed that 12,926 had been sent, only 1533 were intercepted. [redacted] intercepts provide the only coverage of internal nets. There was no change in the systems used by the Romanian Foreign Office during the year. However, the new Communist Foreign Minister had completely reorganized his ministry and was expected to introduce new cryptographic systems at any time. The Romanians used additive enciphered code and the Hagelin machine. Of the Romanian intelligence service, 7029 messages were received and about 2000 translated. Lack of qualified personnel for translation handicapped this project.

Yugoslavia appears to be using the same type of cryptographic system for all its high-echelon traffic. Intercepts numbered 98,654, of which 41,148 were internal commercial plain-text, [redacted] 16,777 unidentified (thought to be military or air), 14,787 air, 2,901 military, and the remainder lowgrade military and police systems or [redacted] Cryptanalytic emphasis was placed on top echelon traffic and solution was achieved in three high-grade systems. Work continued on low grade military, air, and police systems with success in seven cases. Considerable effort was expended on the problem of determining the method of key generation and for a time it looked as if success would be achieved in reconstructing the method. However, this proved a false hope. Recent changes in the top-grade systems in the direction of higher security make it improbable that these systems will be readable in the future.

Of 11,581 intercepts of Albanian traffic, 3,683 were translated and were chiefly valuable as intelligence in portraying the military situation in Greece.

<u>Other European Countries</u>: [redacted] like most other governments whose traffic has been studied by the ASA, have been growing more efficient in their communications. Volume of translations doubled during the year and considerable success was achieved on net recovery [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

were generally readable. The chief new cryptanalytical pro- [redacted] which was just about readable when withdrawn, [redacted] which replaced it. Success in the latter case was made possible toward the end of the fiscal year by an egregious [redacted] For the first time in two and one-half years it would be possible to [redacted]

[redacted]

the most secure types and the least secure. Production figures for 1947 and 1948 are as follows:

	1947	1948
Intercepts	75,658	83,044
Decrypts	36,321	50,799
Translations	12,299	22,213

In addition, approximately 175,000 plain-text messages were processed in 1948.

Intercepts of [redacted] traffic fell off sharply to 80 per cent of the number received in 1947 and 50 per cent of the number received in 1946. This was not the fault of intercept facilities but represents a real decline in the number of

EO 3.3(h)(2)
PL 86-36/50 USC 3605

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

[redacted]

been employing for sometime. Traffic in both these new systems remains scanty.

Current Austrian systems consist of one system introduced in January 1947, made readable in October of that year, and three new ones which are too sparingly used for solution. The Austrians seem not to be cryptologically sophisticated.

Of Portuguese systems, the ASA works only on the [redacted] [redacted] Thirty-eight messages were intercepted and eight decrypted, six being translated. In regard to Spain, ASA's commitment was limited to military and [redacted] [redacted] All military intercept had been provided by the British who discontinued coverage late in Fiscal Year 1947 because of the low grade of intelligence. Only 79 military [redacted] were received during Fiscal Year 1948 and since traffic was so light, no work has been done on these systems.

ASA works only on the military communications of [redacted] [redacted] Except for military and air plain-text message translation, little other work has been done in this connection.

The Near East: The traffic of [redacted] the Near East[21] continued to be studied as heretofore and did not present very serious obstacles to cryptanalytic solution. At the beginning of the year some problems were presented by the fact that headings on the messages as received were in Arabic and therefore could not be read by the logging clerks. Moreover, there was an exceptionally long delay between interception and receipt by the ASA.

[redacted]

In the Arabic group, machine techniques have been used for decrypting [redacted] traffic, thus permitting the personnel assigned to this work to accomplish a greater volume of production. In addition, a few attempts at machine decryption of Iranian material were moderately successful. Afghan systems have proved troublesome owing to very little traffic and daily changes of key.

[21] [redacted]

Production totals for the Near East group in 1947 and 1948 were as follows:

	1947	1948
Intercepted	20,470	35,129
Decrypted	15,429	25,464
Translated	5,827	6,802

The Far East: [redacted] Chinese intercepts of which there were 21,444 in military systems, 51,985 commercial.[22] The three air mission - air attache systems, [redacted] were 80 per cent, 70 per cent, and 60 per cent readable, respectively, but the Joint-Service attache system is unfortunately [redacted] Too little Communist traffic has been intercepted for any serious effort.

Indonesian military traffic contains a considerable number of messages in plain language, together with a variety of cipher traffic. The plain-text material has been studied with profitable results in producing intelligence.

[22] Chinese [redacted] problems were transferred to CSAW at the beginning of the fiscal year.

The Latin-American Group: The traffic of ten South American countries continued to be studied intensively.

Argentina has been using eight active systems, one of

[redacted]

plain-text intercepts were translated or summarized.

Bolivian traffic was virtually 100 per cent readable and intercepts increased 40 per cent. Of a total of 422 code intercepts, 199 were translated or summarized. Also, 1153 plain-text messages were received and 66 translated or summarized.

Substantial progress was made on code recovery (13,605 code values recovered) in the Brazilian systems. Of 3367 encrypted messages received, only one was not decrypted, and 1339 were translated or summarized. Of 3218 plain-text messages received, 132 were translated or summarized.

Chilean systems offered little or no trouble. While there was a decline in the total volume of intercepts, there was an increase in the translatable volume. Encrypted intercepts numbered 4725, of which 4030 were decrypted and 1360 translated or summarized. In addition, the scanning of 1212 plain-text messages produced 34 translations or summaries.

The situation in Colombian traffic is relatively unchanged

EO 3.3(h)(2)
PL 86-36/50 USC 3605

since the last report. Though only 906 encrypted messages were intercepted, 916 decryptions were made during the year and 545 messages were translated or summarized, plus 110 translations out of 5276 plain-text messages received.

The Ecuadorian [redacted]

The Paraguayan system once more must be reported as strongly resisting solution, but only 112 encoded messages were intercepted. A total of only 12 of the 290 plain-text messages received were translated.

Peru presents two code recovery problems and one air [redacted]

The Uruguayan situation remained unchanged; one system is readable and another 90 per cent readable. Only 367 encrypted messages were received and 369 decryptions made during the year, of which 128 were translated or summarized.

There has been an increase in volume of the Venezuelan [redacted] yet only 526 cryptographed messages were intercepted, only four not being decrypted. Two hundred of the decrypted messages were translated or summarised in addition to 117 of the 4676 plain-text intercepts.

Of Central American systems, a new Guatemalan military [redacted] Honduras sent only seven messages; Nicaraguan systems are completely readable, despite the introduction of a new system; Costa Rican traffic is too light; and in the case of Mexico only military attache traffic is received. Traffic from Mexico and Salvador is considerd to be 100 per cent readable.

D. Analysis of Production Figures

In terms of production of intelligence, the following figures furnished by the General Cryptanalytic Branch will be of significance, though they cannot of course be expected to reflect a total perspective of the year's work:

	Total	Monthly Avge.
Intercepts	2,520,097	210,008
Original Messages	2,304,222	192,018
Plain Text	1,502,430	125,202
Encrypted	801,792	66,816
Encrypted Messages:		
In exploitable systems	361,372	30,114
In research	422,435	35,203
Not worked on	17,985	1,499
Messages decrypted	210,119	17,510
Messages Published:		
Plain Text	7,591	633
Encrypted	67,205	5,600

It will be noted that 45.1 per cent of the total number of encrypted messages were in exploitable systems; 52.7 per cent were in various stages of research; while only 2.2 per cent were not worked on, either because of lack of sufficient traffic in the given system or lack of qualified personnel for processing the traffic in question. Of the total number of messages decrypted, 67,205 (or 32 per cent) were published in the Daily Bulletin, the peak of 8,292 for April 1948 being the highest since the war. In addition, a total of 7,591 plain-text messages also appeared in the Bulletin, making a total of 74,796 in all.[23]

A comparison of production figures for the Fiscal Years 1947 and 1948 will be significant in reflecting, to a limited extent, certain trends:

	1947 Totals	1948 Totals
Intercepts	1,534,866	2,520,097
Original Messages	1,294,089	2,304,222
Plain Text	473,918	1,502,430
Encrypted	820,171	801,792
Encrypted Messages:		
In exploitable systems	336,296	361,372
In research	421,411	422,435
Not worked on	62,464	17,985
Messages decrypted	174,271	210,119
Messages Published:		
Plain Text	9,725	7,591
Encrypted	51,540	67,205

Perhaps of greatest significance is the 317 per cent increase in the number of plain-text messages received in Fiscal Year 1948 as compared to Fiscal Year 1947. In fact, there was

[23] The discrepancy between these figures, which were provided by the cryptanalytic units, and those of the Bulletin itself (85,904) are as usual caused (1) by differences in the point at which the count was made, and (2) by different criteria of precisely what constitutes a "message." That is, a multi-part message may be counted either once or by parts.

a five-fold increase in plain-text intercepts during Fiscal Year 1948, with a steady increase from a total of 39,149 messages in July 1947 to 215,428 in June 1948, a peak of 273,888 being reached in April 1948.[24] There was also a 7.5 per cent increase in the number of encrypted messages in exploitable systems and a 20 per cent increase in the number of messages decrypted, despite a 2.2 per cent decrease in the total number received. Not to be overlooked is the 71 per cent reduction in the number of messages not worked on. These are noteworthy achievements, particularly in view of the fact that there was a personnel increase of only 74 in Fiscal Year 1948 as compared to Fiscal Year 1947 (Tab 4).

[24] Approximately 90 per cent of this total increase was for use in the Russian problem. See pages 41 to 44 this report.

CHAPTER IV. SUPPORTING SERVICES

To facilitate the operations described in Chapters One and Two of this report, the ASA continued to employ a large number of people engaged in providing supporting services of three kinds: (1) IBM and other highly-complex machinery, (2) the photographic and secret-ink laboratory, and (3) the information service.

There was a steady continuance in the improvement of techniques for processing cryptanalytic material by IBM machines. The most notable advances were made in the analysis of machine ciphers, in the mass production of cryptanalytic aids for the solution of key-enciphered code systems, and in the development of new devices to perform previously impractical operations. The following new devices, used in conjunction with standard IBM equipment, were put into use during the year: (1) the alphabetic collator, (2) the [redacted] Analogue, (3) the [redacted] Model Generator, (4) the [redacted] Chaining Test, (5) the all-purpose wire-contact relay gate, (6) the tape worksheet, (7) the ASAY-7 Analogue, (8) the Threshold Discriminator, (9) the count device for card-operated typewriters, (10) the checking unit for the binary-arranging device, and (11) isomorphic pattern punching.

Messages decoded by IBM processes came to an annual total of 63,840 in addition to about 2,000 decodes which were produced incidentally to other operations.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

The total number of IBM machines in use during the year remained fairly constant (154). The rental for these was $250,059.30, less than 10 per cent of which was for the swing shift. A total of 64,010,000 cards were used with these machines at a cost of $57,740. Costs for this item rose sharply (44 per cent) in October 1947.[25] A total of $27,417.83 was spent on all kinds of paper used with IBM machines. In addition to the IBM machines just discussed, the ASA constructed in its laboratories a number of special machines for cryptographic and, in an even larger number of instances, cryptanalytic purposes. Among these were the Mathews differencing machine and the mononomedinome reader, used successfully on Balkin Traffic.

Turning now to the highlights of research and development activities of the Agency, work was started on a new type of endeavor, represented by developments such as the cipher machine setting generator, an attempt by pure research to push forward the frontier of knowledge in regard to cryptanalytic principles of rotor devices when applied to unpredictable motions. Many promising fields of theoretical research have been stopped because of the impossibility of mathematically predicting their results. This machine will compute and chart such motions which cannot be calculated and may eventually derive new mathematical concepts capable of predicting these

[25] From $0.66 to $0.95 per thousand.

very important statistics.

In the electronic field, a start has been made on a general purpose cryptanalytic aid which, because of its high operating speed and versatility, could be used on a multiplicity of cryptanalytic problems. An electronic tape comparator was the result of this study, and by using perforated teletype tape operating at speeds of 5,000 to 10,000 characters per second ASA has promise of a very useful cryptanalytic tool.

In the field of photography and secret inks, new facilities were introduced on a limited scale for the development in laboratories at Headquarters, ASA, of color transparencies made by photographing classified material which could not be sent to the manufacturer for processing, as is the usual procedure with unclassified films. A strike of ITT communications workers affecting one of the Shamrock sources resulted in a serious curtailment of traffic from January to March 1948 but production has since been brought back to normal. Attempts were made to determine the degree of reconstruction of rotor wirings which could be made from a photograph of a rotor and it was found that 80 per cent of the wiring could be recovered. On several occasions, the facilities of the laboratory were called upon by counterintelligence agencies to effect surreptitious entry into the mail of persons under surveillance by those agencies. On each occasion, successful entry was made and the contents subjected to routine examination which included complete photostating. Tests were made of two substances

EO 3.3(h)(2)
PL 86-36/50 USC 3605

easily available in the field (atrabine and halazone, used for anti-malaria and water purification purposes) to determine whether they could be used for secret-ink materials, but the tests proved that those substances were unsatisfactory because they were too easily detected. Research on other materials of this kind continues. The German secret-ink testing machine known familiarly as the "Wurlitzer Organ" was after complete study disassembled and some parts retained for miscellaneous uses. For the Atomic Energy Commission a special fluorescent marking ink was developed for identifying photographs and documents. Research was also conducted on the problem of [redacted] with a view to reducing the time required which formerly was the major part of a day. After several unsuccessful attempts, quick-setting alloy amalgams provided a satisfactory answer to the problem. [redacted] have been made in from two to three hours and the reproductions are of a high quality. Charred documents from the destruction of cryptomachines were studied for possible readability and recommendations for improving destruction technique were made.

Some idea of the extent to which the information service assisted in accomplishing the results mentioned in preceding sections by supplying collateral information will be obtained from noting that during the year a total of 37,185 requests for data were answered, and 149 special publications and reports were made, in addition to supplying 5,808 footnotes to messages which appeared in the Daily Bulletin. Collateral information from other sources was of particular value in connection with the plain text problem. Not only were the staff and operating divisions of ASA provided with collateral information, similar services were extended to CSAW, ID, Special Projects Section of the State Department, USAF, and CIA.

COPY ~~TOP SECRET~~ [illegible]

[illegible]
6200342
7102051

AS TO AS-20 27 Mar 47

Policy Governing Development of Cryptologic Equipments which are to be Issued to Echelons of Command below Division Headquarters

Major Bergman 462

1. The policy set forth below has been approved and will be adopted at once:

> "These cryptologic considerations dictate the necessity therefor, a new item of communication security equipment intended for issue to echelons of command below Division Headquarters and corresponding Air Force units will be provided with two types of crypto components--one for use in the equipment when issued for field testing, training, or maneuvers, and the other for use in the equipment when needed and issued for emergency situations. The latter component will be given special protection prior to issue."

2. It is desired that recommendations be submitted to this office on any proposed low echelon device as to whether a training component is considered necessary under the above policy, listing those cryptologic considerations from which the recommendation is drawn.

3. The MX-519A has been proposed as a device to fulfill the interim need for a BMR III and IV device. Inasmuch as BMR IV is defined in SIGTRA as a small cipher machine for use by field units down to and including battalion headquarters, the policy set forth in paragraphs 1 and 2 above applies.

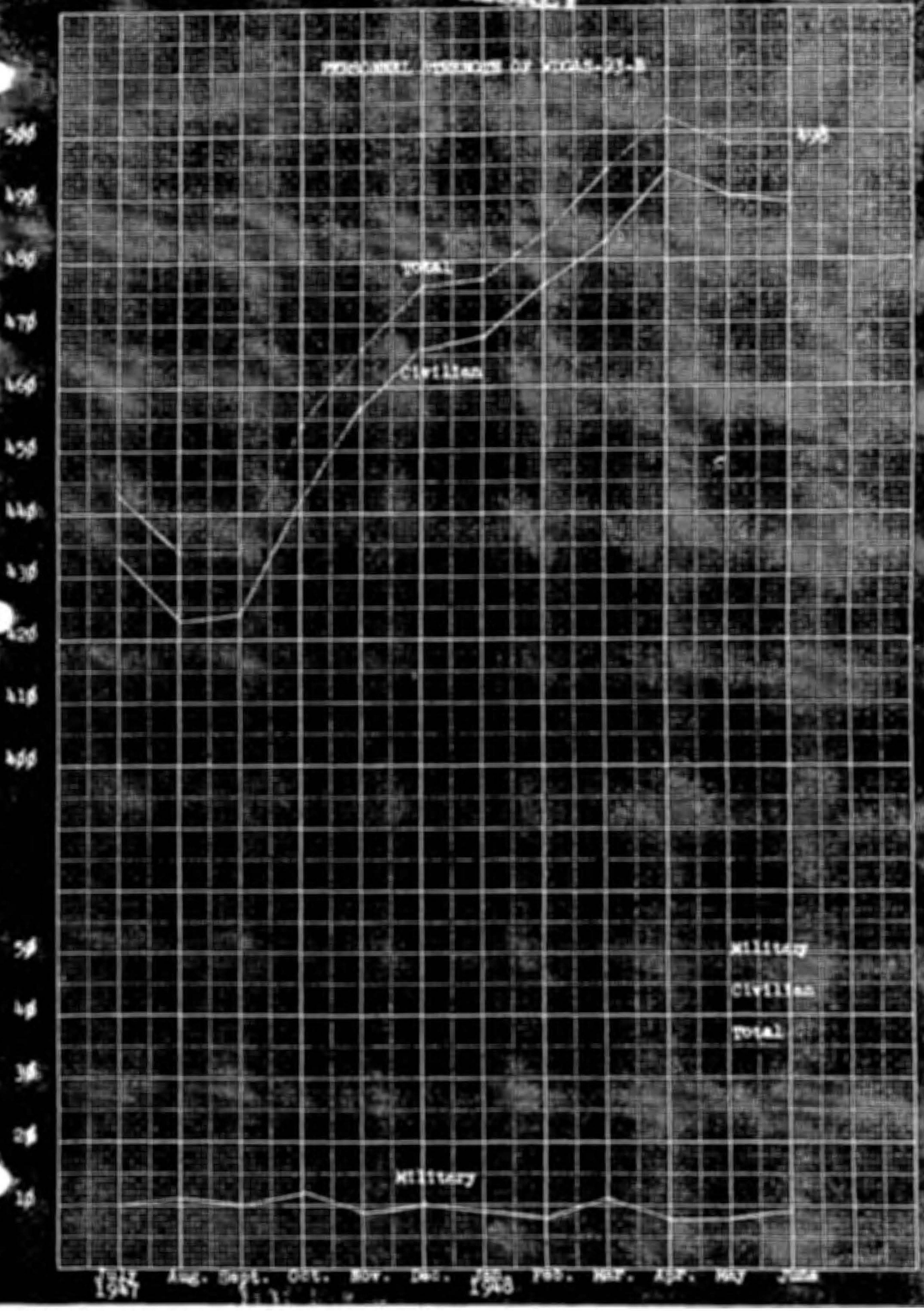
GEORGE A. BICHER
Colonel, Signal Corps
Deputy Chief, Army Security Agency
Ext 498

Copy Furnished
AS-14
AS-80
AS-90

C
O
P
Y

~~TOP SECRET~~

TOP SECRET

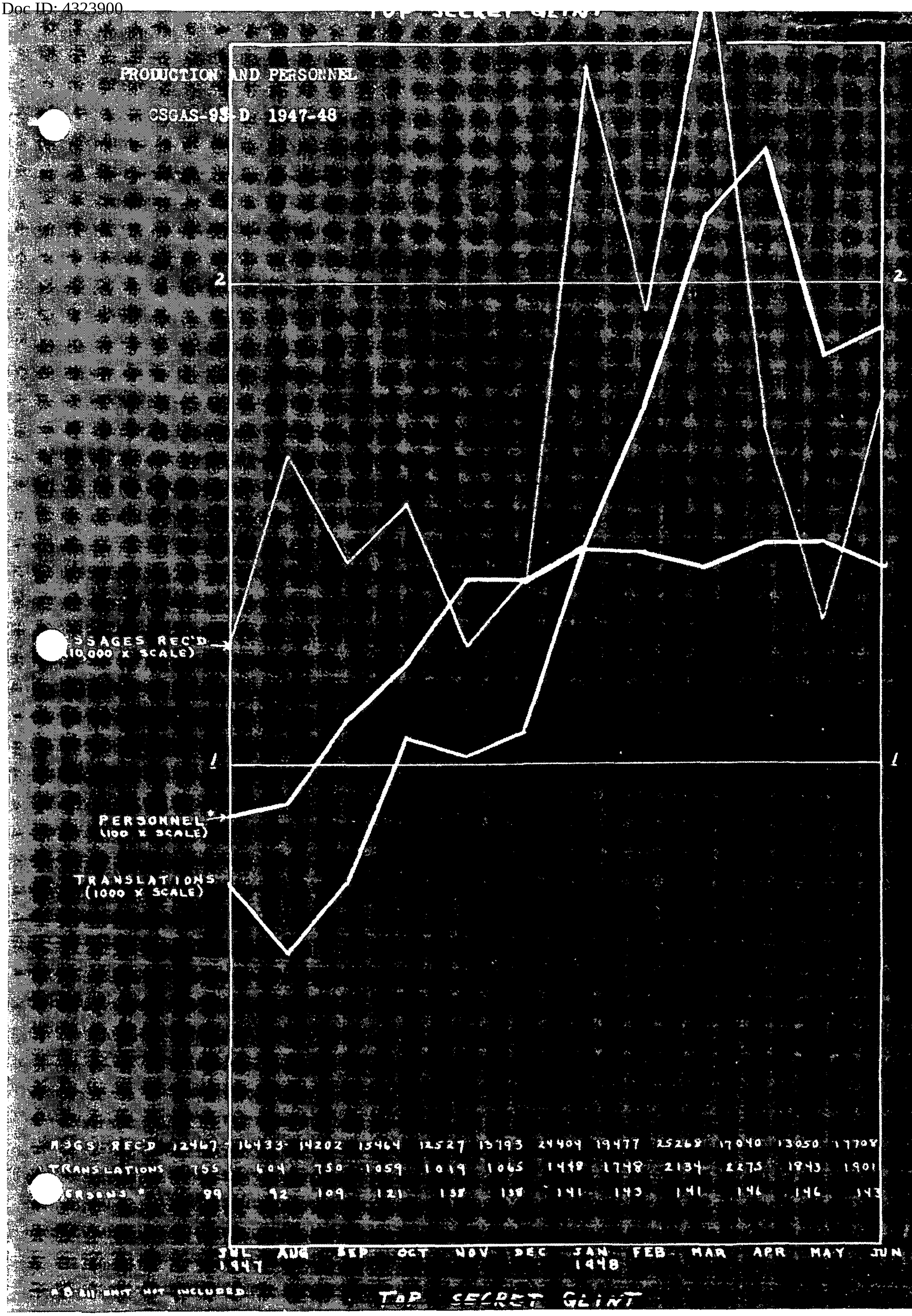


PERSONNEL STRENGTH OF WDGAS-93-B

7102051

PRODUCTION AND PERSONNEL

CSGAS-93-D 1947-48



	JUL 1947	AUG	SEP	OCT	NOV	DEC	JAN 1948	FEB	MAR	APR	MAY	JUN
MSGS REC'D	12467	16433	14202	15464	12527	13793	24409	19477	25268	17040	13050	17708
TRANSLATIONS	755	604	750	1059	1019	1065	1448	1748	2134	2275	1843	1901
PERSONS *	99	92	109	121	138	138	141	143	141	146	146	143

* A D-211 UNIT NOT INCLUDED

7102051

COMPARISON OF OPERATIONS DIVISION (CSGAS-90)

PERSONNEL FIGURES FOR FISCAL YEARS 1947 AND 1948

	CIVILIAN		MILITARY		TOTAL	
	1947	1948	1947	1948	1947	1948
Jul	1459	1491	77	73	1536	1564
Aug	1402	1474	115	67	1517	1541
Sep	1333	1463	99	68	1432	1531
Oct	1328	1507	150	68	1478	1578
Nov	1294	1543	129	65	1423	1608
Dec	1286	1548	129	63	1415	1611
Jan	1307	1573	143	67	1450	1640
Feb	1462	1575	158	67	1620	1642
Mar	1547	1570	104	67	1651	1637
Apr	1538	1553	83	62	1622	1615
May	1503	1537	74	63	1577	1600
Jun	1495	1549	71	61	1566	1610
AVERAGE FOR YEAR	1413	1532	111	66	1524	1598