



governmentattic.org

"Rummaging in the government's attic"

Description of document: National Security Agency (NSA) document: A History of U.S. Communications Security Post World-War II – released under Mandatory Declassification Review (MDR)

Released date: February 2011

Posted date: 07-November-2011

Source of document: National Security Agency
Declassification Services (DJ5)
Suite 6884, Bldg. SAB2
9800 Savage Road
Ft. George G. Meade, MD, 20755-6884

Note: Although the titles are similar, this document should not be confused with the David G. Boak Lectures available:
http://www.governmentattic.org/2docs/Hist_US_COMSEC_Boak_NSA_1973.pdf

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

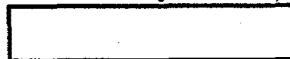
~~COMINT~~

**A HISTORY OF U.S. COMMUNICATIONS SECURITY
POST-WORLD WAR II**

by

? Ed Fitzgerald ?

P.L. 86-36



Declassified and approved for release by
NSA, NSC, OSD, the Joint Staff, DIA, the U.S.
State Department, the U.S. Army, the U.S.
Navy, and the U.S. Air Force on 02-04-2011
pursuant to E.O. 13526, MDR 59142

~~SECRET~~

~~COMINT~~

~~SECRET~~

Acknowledgements

The sources used in compiling this history are many and varied. We are especially indebted to Mr. George Howe, NSA Historian from 19 to 19 , for the significant contributions he has made to the Agency's heritage in his five volume draft of *The Narrative History of AFSA-NSA*.

The portion of the History covering most aspects of wired rotor development is based on A *Survey of Wired Rotors* which was prepared by a long time expert in that field, Mr. Ryan Page. Mr. Page's survey is presently being reviewed and updated, and will be published in due course as an adjunct to this History of Communications Security. Additionally, an extensive work by [redacted]

[redacted] of NSA's R&D organization, on secure voice equipments and techniques, covering the years to , has been used as a springboard for the limited entries herein on secure voice matters.

This work will be published at some future date also.

P.L. 86-36

A third and most important historical study in tracking the development of critical equipments used in the communications security area was also prepared by [redacted] in 1967.

This work reviews the major technical and managerial problems which were encountered in the development of a wideband voice security system for tactical airborne, vehicular, and manpack applications. This program covered about twenty years and resulted in the highly acclaimed TSEC/KY-8, FY-28, and KY-38 systems. This historical study will also be published in due course as a further adjunct to this History.

Many thanks go, also, to the numerous past and present employees of the S Organization for their valuable advice and assistance.

~~SECRET~~

~~SECRET~~

Foreword

In his treatise entitled "The First SIGINT Organization,"¹ Mr. Bill Millward, a former member of the Directorate of GCHQ,² described the scene in Henry V, Act II, Scene II, which showed Shakespeare's awareness of the possibilities of SIGINT. In that scene, a conspiracy led by the Earl of Cambridge is unmasked when a Lord, in an aside, observes that "the King hath note of all that they intend, by interception which they dream not of." The King addresses the conspirators, and hands each one a slip of paper purporting to be a commission. Each, upon reading his paper, turns pale and falls to his knees, pleading forgiveness. According to Mr. Millward, the slips of paper were quite likely bits of SIGINT end-product based on the King's interceptions.

This story is important because it dramatizes what may be the first known, documented, unequivocally recognizable absence of prudent communications security practices. Had the conspirators the good sense to apply COMSEC principles to their conspiratorial notes, writs, letters, and other communications, and thereby prevented the King from learning of their plots, there is no way of knowing what effect their dastardly actions might have had on Henry V's reign nor on Shakespeare's telling of it.

For all of that, it was still many years before the art of communications security reached the point of being a much used and accepted tool.

¹Contact, 19 .

²Mr. W. Millward, C.B., C.B.E. was formerly Director of Requirements at GCHQ

~~SECRET~~

~~SECRET~~

Introduction

The history of the invention, development, and application of cryptographic devices, machines, and associated apparatus and material is long and interesting. Attempts to keep secure the contents of the various communications passing between and among civil and military ^{organizations} ~~factions~~ have gone through many vicissitudes over the years, not always with a great deal of success. This is evidenced from the earliest days in the observations of Sir Francis Bacon who, in 1623, noted that "...many times the greatest matters are committed to future and weak ciphers."¹

Until the advent of electronics/cipher machines, most cryptographic devices were built upon or around concentric circular rotating numbers such as cipher wheels, cipher discs, etc. One of the earliest developments of such devices appeared in Italy around 1470 in a paper written by an Italian cryptologist named Alberti. There were a few modifications made from time to time, but the basic methods of trying to keep

¹In Gilbert Watts' translations (1640, p.270) of Bacon's De Augments Scientiarum, London, 1623, made from time to time, but the basic methods of trying to keep the underlying plain text communications "secure" remained.

Progress in the development of cryptographic equipments and devices kept pace, and apparatus for protecting all manner of communications were developed and continually perfected. These included machines and keying devices to secure literal communications -which employed letters of the alphabet; cifax transmissions--which were picture or facsimile transmissions; and ^{ciphony?} ciphone transmissions--telephonic transmissions.

Early twentieth century communications security devices, such as those used up to the 1930's, had been based primarily on manual techniques. This included code books, transposition processes, auxiliary devices for use with printed tables and books, strip-ciphers, and similar processes for disguising plain text messages. Additive tape machines had been used to a limited degree. A few mechanical (i.e., non-electrical) ciphers such as the German Kryha and the Hagelin devices had appeared but had been employed only very selectively or not at all by the U.S.

1 ~~SECRET~~

~~SECRET~~

Enciphering and deciphering were tedious, time consuming processes. The wired rotor, which became practicable for secure machines in the late '30s, was to revolutionize the encryption/decryption processes of the era.

By early 1942 rotor machines were beginning to ease the load on manual systems and to lower the time between filing of a message and delivery to its intended recipient. At least this was true for major military bases. As World War II progressed, rotor machines became the backbone of the cipher networks at fixed plant levels for Army and Navy alike. (The Air Force had not yet been established as a separate service.) The use of rotors continued to grow through the 1940's and early 1950's. About that time techniques to supplant rotors became practicable and affordable. Miniature tubes came first, followed closely by magnetic binaries (BI-MAGS) and transistors. Development of these, and of the later miniaturized technologies, spelled the eventual end for rotors in U.S. Cryptography.

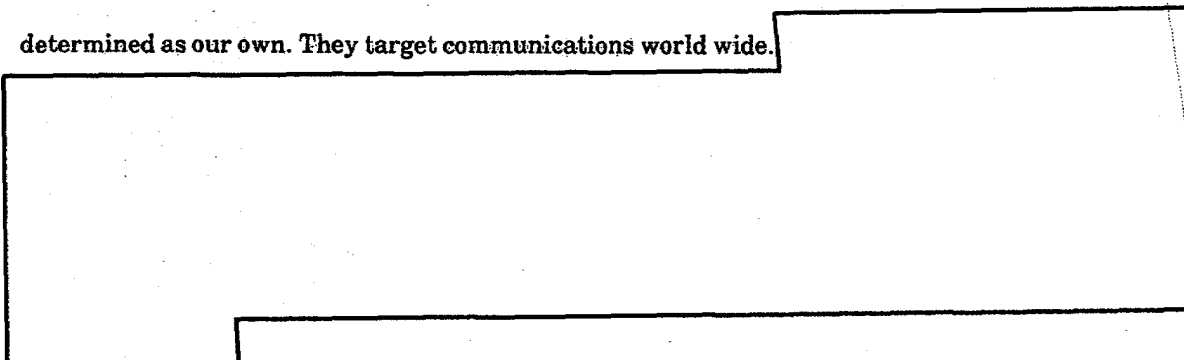
Title

— Begin

Even in the light of rapidly advancing technology, keeping our communications secure continues to be a difficult and challenging task. We have been eminently successful so far, and our goal is to maintain that status.

EO 1.4.(c)
P.L. 86-36

There are a number of reasons why this task grows even more difficult. For one, the Soviet Union has a very efficient SIGINT service which we must consider to be as dedicated and determined as our own. They target communications world wide.



Another reason is that our exposure of communications signals increases regularly. The U.S. government transmits millions of messages each month. These are sent in various transmission modes, teletype, morse, telemetry to and from missile and satellites, radiotelephone,

2 ~~SECRET~~

~~SECRET~~

commercial (radio, television data), etc. The volume of material in the radio frequency spectrum which is subject to intercept by anyone with the proper receiving equipment is staggering, and it is increasing. The job of providing communications security on this scale is, to say the least, a big and challenging one.

3 ~~SECRET~~

~~SECRET~~

Chapter 3

Part I. The Elements of Communications Security

Most members of the cryptologic community have a fairly good knowledge of what the term communications security means. But just in case there are some who do not, communications security (COMSEC) can best be defined as being the natural and direct defense against communications intelligence (COMINT). Just as communications intelligence has three elements, cryptanalysis, traffic analysis, and the use of information picked up through normal intelligence channels, so also does communication security have three distinct elements, i.e., cryptologic security - the defense against cryptanalysis; transmission security - the defense against traffic analysis; and physical security - the defense against espionage and other intelligence gathering means. Putting these three defenses together gives a working definition of communication security, which can be stated simply as being "the sum of all of the measures necessary to deny to unauthorized persons the possibility of deriving intelligence from one's own communications." Actually, communication security is the state which results from successfully implementing all these measures, so it can be described as one active thing, i.e, something which is done; and also as an inactive thing, i.e., a condition which is achieved.

The following is a broad summary of how the whole field of communication security was controlled and how it operated during the period after World War II and for the years up to about 1955. In the mid-1950's, major technological advances resulted in major changes in the mechanical and manual aspects of communication security, but certainly not in the philosophical bases of this vital responsibility. It is important to note that during this time communications security measures in the U.S. were applied almost exclusively to communications of the military services and of the State Department.

The elements which comprise communications security are:

4 ~~SECRET~~

~~SECRET~~

Cryptographic Security - This consists of the provision of cryptographic systems which inherently secure; provision of the rules, regulations, and policies to govern their use; and the execution of proper measures to insure their correct use.

Transmission Security - This is the part of communications security which results from all measures designed and activated to protect transmissions from interception and traffic analysis.

Physical Security - This amounts simply to taking the necessary precautions to ensure physical protection of crypto equipment or material.

Up until the mid-1950's, the process of achieving cryptographic security usually began with a requirement. This could be submitted by one of the military services, or by all services jointly. The requirement stated the need for a secure cryptographic system to fill a particular communications need. It stipulated certain specifications to be met, certain desired characteristics as to speed, reliability, and security, and perhaps others such as size and weight. If the requirement could be met by existing cryptosystems, the proper materials would have been provided and the job was relatively simple. But if it was a new requirement, a newly expressed need which had not arisen before, a different procedure was called for.

a. Requirements, Production, Control. First, a research project would be established. Engineers would devise an equipment which would meet the physical requirements; cryptographic experts would "invent" a cryptographic component which would fit into the geographical limitations imposed upon them, and one which would afford the necessary degree of cryptographic security, one which would resist cryptanalytic attack by other COMINT organizations. When this was completed, the project would usually be turned over to an outside commercial development company. Here the fine points were completed, development models made and tested, and the specifications and designs for mass production established. Following this a production contract was let, the manufacturer tooled up for the job, and the first production models were provided. These were then turned over to the originators of the initial requirement, and they would conduct service tests. As a result of the tests, production modifications were made if necessary, and the

5 ~~SECRET~~

~~SECRET~~

equipments were then produced. Thus, in keeping with the definition of cryptosecurity through the first step, provision of an inherently secure system was completed.

While the production of basic equipment was going ahead at some commercial plant, AFSA/NSA was manufacturing, in its own facilities, the materials that had to be provided with the equipment. As was generally the case, most cryptosystems consisted of a basic, unvariable method of operation, usually a machine and, in addition, certain variable elements. It was these latter variables which were produced by AFSA/NSA. Usually they consisted of cipher rotors, small wheels with electrical circuits through them, which could be placed in a cipher machine in a large number of ways and which performed the actual process of encipherment. These would be accompanied by key lists, printed sheets which told an operator how he was to arrange his variable elements for the message he was to encipher.

The bulk of the manufacture of this type of material was done by the cryptologic agency, with commercial assistance. For example, blank rotor shells were produced outside, but the wiring and all other security features that went into a completed rotor were inserted at AFSA/NSA.

The next step in the birth of a new cipher system had really been going on all the time. Various ways of using the system had been under study and finally a procedure for its use had been decided upon, a procedure which would maintain the inherent security of the system and at the same time be as simple and easy on the operator as was possible. This procedure was then written up and printed as a document which went to each user of the system. Also published were statements of policy on use of the system physical security regulations that had to be observed in its use, and other general rules governing its employment.

At that point everything was turned over to the services, machines, rotors, keylists, etc. The first set of material was usually especially made for training, and the services trained their cryptographic technicians in the new system. The operational material was then distributed to the users, an effective date was promulgated, and the new system was put into operation. Once it was in use the services were responsible for seeing that the rules were properly followed. In order to insure that proper action was taken when serious mistakes occurred, a violations reporting

6 ~~SECRET~~

~~SECRET~~

procedure was put into effect. This consisted of a requirement that any command or service element noting a mistake in an encrypted message, or learning of a violation of physical security, had to make a report to the proper authorities citing the circumstances. The case was then evaluated in terms of cryptanalytic significance, and the sending organization was informed of the action which had to be taken. In all instances AFSA/NSA was responsible for determining the effect of the violation for determining the effect of the violation and for determining what correct action would be taken in the way of superseding a system, correcting a procedural deficiency, or clarifying existing instructions. Other actions to prevent recurrence, improved training, disciplinary action, improved supervision, etc., were primarily users (mainly military services) responsibilities.

Closely interwoven in this pattern of control was cryptosecurity's companion element, physical security. Physical security of cryptomaterial breakdown into three main aspects - establishment of safeguards governing the material itself i.e., how it should be protected in transit and while in use and what accounting records needed to be maintained on it; safeguards governing protection of the area in which it was used, i.e., what kind of facilities had to be provided, guards, barred windows, limited access, etc.; and safeguarding against personnel defections and carelessness by the establishment of personnel clearance provisions. In all of these AFSA/NSA established the standards considered necessary; they were usually the minimum standards, however, and the military services were at liberty, in most cases, to institute their own more restrictive rules if they so desired.

The transmission security (TRANSEC) element of communication security was and is as critical to the system as was the cryptographic and physical security aspects. Transmission security is best defined as the taking of all measures necessary to protect communications from unauthorized interception, traffic analysis, and initiative deception. There is no absolute defense against interception because almost anything that is transmitted can be intercepted. But there are some means of transmission which can be much more difficult to intercept than others. Therefore, when "measures necessary to protect communications from unauthorized interception" are used,

7 ~~SECRET~~

~~SECRET~~

~~COMINT~~

what is really meant is the execution of steps designed to make interception as difficult as possible.

Included in these protective measures are:

- 1) the use of specialized radio equipment, special antennas, frequencies, etc.
- 2) protected landlines
- 3) registration of and accounting for, documents and equipment
- 4) specialized transmission, i.e., infra-red, laser, etc.
- 5) monitoring of friendly communications circuits for security supervision.

EO 1.4.(c)
P.L. 86-36

Transmission security is, then, what is done to prevent loss of intelligence from the external message characteristics by protecting the signal during the act of communicating.

New developments in communications techniques and in communications security equipments and procedures started to appear in strength beginning around the mid-1950's. Generally speaking, cipher systems up till then had been of three kinds, manual systems with encryption done entirely by hand; off-line machine systems in which encryption was done mechanically with the result still left to be transmitted; and non-line teletype systems in which encryption took place simultaneously with transmission. We had reached a peak in this latter kind of development by 1954-1955. One new off-line cipher machine had just been given its final service test and was in production, and others were just a few months away. But even those new units, which were basic systems for the next six or seven years, were geared to more-or-less old fashioned concepts of communications.

The first new concept, not new really but certainly in the early to 1950's just beginning to see the light of day as an actuality, was fully automatic switching equipment at relay centers. Relay installations of that era consisted of a line receiving circuit, a typing reperforator which

~~SECRET~~

produced the received message, and a teletype transmitter for each send channel which read the perforations on a tape introduced into it and caused the tape to be transmitted to the appropriate receiving point or next relay station. The gap between receive reperforator, and teletype transmitter was spanned manually. The purpose of the newly introduced equipment was to span it automatically, to transfer messages from receive point to transmit point electrically without any requirement for handling messages physically.

Automatic equipment which was designed and became available in that period was capable of checking incoming channel continuity numbers, recognizing message precedence and routing information, and automatically transmitting messages via cross-office circuits to the correct outgoing circuits. The demand for strict communications security complicated all of this, since cryptographic equipment associated with the relay equipment also was required to provide an equal degree of automaticity, and this was quite difficult to achieve. The signals transmitted as switching information, that gave precedence and routing "instructions," had to be in plain, unencrypted form in the switching centers. Therefore, the principle of "link encryption" was adopted. This meant that a message, automatically encrypted at its point of origin, was automatically decrypted, routed to the proper outchannel, and reencrypted at each relay point. The circuits between relay points were in constant use, with an enciphered signal continuously transmitted whether intelligence was being transmitted or not. When a message was entered into the system everything, heading and all, was encrypted. Thus, an almost perfect answer to traffic analysis had been devised. On circuits such as these, it was impossible for interceptors to detect the existence of messages, and the first traffic- analysis tool, volume count, disappeared. The other tricks of the trade, routing instructions, precedence information, call signs and the like were equally absent.

But the development problem was by no means licked. There was not an entirely suitable switching equipment, nor did any of the contemplated ones permit, without some basic changes, association with cryptosystems believed to be workable at that time. It was a long while, into the late 1950's, before completely secure automatic relay arrangements were in operation.

9 ~~SECRET~~

~~SECRET~~

Chapter I

Service COMSEC Establishments U.S. Army

Part II

COMSEC 1945-1955

At the beginning of World War II, the Signal Security Agency's Code Compilation Section was responsible for the preparation and administration of cryptographic systems designed to protect the communications of the United States Army from attack by enemy cryptanalysts.¹ These tasks included:

- compilation of codes
- preparation of manual cipher systems
- design of machine cipher systems, and supervision of their development and production.
- preparation of keys for encipherment of codes and for use with cipher systems.
- distribution, accounting, and other control features.

¹ History of the Signal Security Agency (forerunner of the Army Security Agency), Vol. VIII, Chap. 1.

security studies and monitoring of traffic.

During the war, technological advances tended to bring about the replacement of both codes and manual ciphers by the increasing use of cipher machines, some of which had been developed prior to the conflict, but many of which were new types developed during the war.¹

In protecting against enemy SIGINT operations, the Signal Security Agency's goal was to develop machinery and techniques which would effectively prevent all possibility of obtaining useful intelligence from any Army communications. In retrospect, the experience of many years of the cryptographic art proves attainment of that goal to be most difficult, if not impossible. Indeed, at that time even relative security was regarded as high achievement.

At the end of World War II, Army communications security was the sole responsibility of the Signal Security Agency. The head of the Signal Security Agency at that time reported to the Army Chief Signal Officer on matters relating to COMSEC.²

On 15 September, ⁹¹⁵ a new organization, the Army Security Agency (ASA) was established.¹ This Agency operated under the direct command of the War Department and comprised all signal intelligence and communications security establishments, units, and personnel that were then attached to major forces, commands, and departments, or their subordinate elements. There were no changes made in the location of units or personnel, but the all inclusive instructions from the War Department applied to a diverse assemblage of operational activities, including the Signal Security Agency; Second Signal Service Battalion personnel engaged in SIGINT activities; Signal Radio companies; Signal Intelligence Service Detachments; Army Air Forces mobile radio

¹Ibid.

²When wearing his other hat, i.e., COMINT, the Chief, Signal Security Agency reported to the Assistant Chief of Staff, G2.squadrons: Radio Intelligence Platoons of Aviation Signal Companies; and all other units and activities organized to perform communications intelligence and communications security functions.

At the time of this change in structure, COMINT and COMSEC units and personnel of ASA were allocated to major

~~SECRET~~

WAGO 322, (4/9/45), OB-S B-M, dated 6 September 1945. (S) forces and commands as needed to meet local tactical or security requirements. When so allocated, such units and personnel were administered by the major force or command, but operated in accordance with directives issued by the Chief, Army Security Agency. In addition, other units of the Army Security Agency were placed in the territories assigned to a major force or command in order to meet other than local tactical or security requirements. In those cases the units and personnel were administered by the major force or command but were operationally under the direct command of the War Department, through the Chief, ASA.

As head of this new establishment, the Chief, Army Security Agency, was responsible for the following SIGINT, and COMSEC activities.

- a. Interception, identification, and analysis of radio and wire traffic.
- b. Organization, employment, and operation of COMINT and COMSEC establishments, procedures, and equipments within the Army, exclusive of message centers.
- c. Research and development of all items of equipment of particular interest to the Army Security Agency.
- d. Determination of the military characteristics of and the requirements for items of equipment peculiar to the Army Security Agency.
- e. Research, development, preparation, publication, revision, storage and distribution of all cryptographic equipment and material (including codes, ciphers, and secret inks) required by the Army; the establishment of procurement requirements and accounting for such equipments; and the maintenance of liaison with other agencies in connection therewith. The Army Security Agency was authorized to delegate such of those duties and responsibilities as appropriate to its field units or to major forces or commands.
- f. Cryptographic and transmission (radio, wire, and courier) security.
- g. Organization and training of all units, detachments, or teams, and training of all individual specialists assigned to ASA.

12 ~~SECRET~~

~~SECRET~~

h. Determination of doctrines, techniques, and the preparation of field manuals and training literature.

i. Preparation of T/O's, MOS's, etc, required by the Army Security Agency.

j. Establishment of personnel requirements and personnel policies in accordance with War Department policies.

k. Review of instructional programs in service schools engaged in training clerks, technicians, and other specialists involved in all phases of cryptographic work.

The Chief Signal Officer of the Army, who prior to the establishment of ASA had directed many of the activities which were performed by the Signal Security Agency was made responsible for providing communication facilities needed by ASA to and between forces and commands overseas. Major force commanders abroad were instructed to provide adequate communication facilities to the ASA units within their respective commands.

All facilities, equipments and records used in the operation of the ASA units and personnel, and the appropriate funds for these, were transferred to the Army Security Agency. ASA was, therefore, a strong, well organized and well managed signal intelligence arm of the U.S. Army. It stayed in this basic alignment until 1 January 1949 when certain communication intelligence and communication security functions were transferred from the Department of the Army to the Department of the Air Force and were incorporated into a newly established United States Air Force Security Service.

B. The U.S. Air Force

When it was established in 1947, the Department of the Air Force instituted a practice of routine communications security activities organically associated with the operation of its communications networks. Unlike the Army and the Navy, the Air Force, up until 1 January 1949, did not have any single entity responsible for directing and coordinating all phases of communications security. The Department of the Army undertook to provide these services to the Army Air Forces in accordance with the terms of a 15 September 1945 letter signed by MGen Edward F. Witsell, Acting Adjutant General, U.S. Army.¹ The first formal step in establishing the

~~SECRET~~

USAF Security Service was taken on 20 October 1948, as noted in the following excerpts from the directive of the Air Force Adjutant General:

AFOIR-SR322

20 October 1948

Subject: Functions of the USAF Security Service

To: Commanding Generals, Major Air Commands in ZI and overseas.

1. The USAF Security Service, established with headquarters at Arlington Hall, Washington, D.C., on

1AGO 322 (4/9/45) OB S-M-B. dated 6 September 1945 (S) 20 October 1948, will operate under the direct control of the Chief of Staff, USAF (such control to be exercised by the Deputy Chief of Staff, Operations, through the Director of Intelligence.

2. There will be assigned to the USAF Security Service as field units thereof all communication intelligence and communication security establishments, units, and personnel not otherwise assigned by Headquarters, USAF.

3. Personnel will not be transferred to or from the USAF Security Service, to or from any field unit thereof, or to or from any otherwise assigned communications intelligence and communication security unit without prior approval of Headquarters USAF in each instance.

4. Communication intelligence and communication security units and personnel of the USAF Security Service will be attached to major air commands in ZI and overseas as needed to meet security and tactical intelligence requirements.

5. Other communication intelligence units and/or personnel of the USAF Security Service may be located in the territory assigned to a major air command in ZI or overseas in order to meet other than local intelligence and security requirements.

6. The USAF Security Service will be responsible for the following communication intelligence and communication security activities:

~~SECRET~~

- a. The operational command and direction of all communication intelligence and communication security units and personnel assigned to the USAF Security Service.
- b. The interception and traffic analysis of foreign tactical type traffic of interest to the Air Force and for the location and identification by electrical means of stations passing this traffic.
- c. The cryptanalysis of intercept which is exploitable in the field.
- d. The preparation and coordination of military characteristics and operational requirements and coordination of the research and development of communication intelligence and communication security equipment.
- e. The preparation, and publication of key lists and related items for use with Air Force cryptographic systems.
- f. The storage, distribution, and accounting for all cryptographic systems and equipment held by the Air Force. Existing facilities and procedures will be used where feasible.
- g. The preparation of operating and maintenance instructions for cryptographic equipment and related systems developed and used exclusively by the Air Force; collaboration in the preparation of operating and maintenance instructions for jointly developed and used cryptographic systems and equipment. Security classification of the aforementioned equipment and related systems will be a responsibility of the Agency developing the equipment.
- h. The cryptographic and transmission security of Air Force communications.
- i. The establishment of requirements for personnel for the communication security units in accordance with established Air Force policies.
- j. The organization and training of all units and provision for the specialized training of all individuals engaged in Air Force communication intelligence and security activities.
- k. The determination of doctrine and techniques and the preparation of training literature and field manuals.

~~SECRET~~

l. The preparation of Tables of Organization and Equipment, Military Occupational Specialties, and related items peculiar to the activities of the USAF Security Service.

m. The budgeting for Air Force cryptographic equipment and for the necessary expenditures in the discharge of the communications intelligence and communication security activities.

7. The Director of Communications will exercise staff supervision at the Headquarters USAF level over all matters pertaining to cryptography and communications security in coordination with the Director of Intelligence.

8. Communications facilities required by the USAF Security Service will be provided by the Director of Communications.

9. The troop basis of major air commands in ZI and overseas will reflect any transfers effected under the provisions of this letter.

10. For purposes of security, knowledge of the activities in which the communication intelligence units are engaged will be confined to only those individuals whose official duties require such knowledge. Dissemination of intelligence produced will be made only to those selected individuals who have been cleared for Special Intelligence.

By Command of the Chief of Staff

(signed) L. L. Judge

Colonel, USAF

Air Adjutant General

On 31 December 1948, Joint Army and Air Force Adjustment Regulations No. 1-11-54, signed by Omar N. Bradley, Chief of Staff United States Army, and Hoyt S. Vandenberg, Chief of Staff United States Air Force, delineated the role of the new USAF security service element that would accept the transfer of certain COMINT and COMSEC responsibilities from the Department of the

~~SECRET~~

Army.² Effective 15 February 1949, the Air Force assumed responsibilities for the following functions:

²JAAFAR 1-11-54, 31 December 1948

2. Preparation and publication of operating and maintenance instructions for cryptographic equipment and systems developed by, and used exclusively by, the Air Force.

3. Collaboration in the preparation and publication of operating and maintenance instructions for cryptographic equipment and systems in which both the Army and Air Force are involved in the use or development thereof.

4. Determination of doctrines and techniques, and for the preparation of training literature for Air Force COMINT and COMSEC operations, with the exception of individual specialists training conducted by the Army for the Air Force.

5. Preparation of Tables of Organization and Equipment for USAF COMINT and COMSEC units.

6. Budgeting for:

a. cryptographic equipment purchased for the Air Force by the Army.

b. COMINT and COMSEC activities for which the Air Force is responsible under the reference agreement.

c. Civilian and military personnel and other costs necessary for the conduct of the functions transferred.

7. Production, dissemination, and proper handling of departmental special intelligence for the Department of the Air Force.

8. Operation of fixed and mobile intercept stations assigned to the Air Force.

9. Transmission security of United States Air Force Communications.

10. Participation in activities which are performed by ASA as a common service, i.e.,

a. traffic analysis

17-~~SECRET~~

- b. cryptanalysis
 - c. research and development
 - d. development of common COMINT and COMSEC doctrine
 - e. preparation of common field manuals and training literature
 - f. certain training activities carried out by the Army Security Agency.
- 11. Interception and traffic analysis of:
 - a. tactical traffic of interest to Air Commanders in the field.
 - b. weather traffic
 - 12. D'Ping and identifying by electrical means stations passing traffic of interest.
 - 13. Field exploitation through cryptanalysis, where possible.
 - 14. Research, development and procurement of Air Force COMSEC equipment.
 - 15. Training of personnel and integral units in COMINT and COMSEC specialties.

Although the Air Force was also assigned direct responsibility for cryptographic security of USAF communications, preparation and production of key lists, and storage, distribution and accounting of cryptographic systems and equipments, the Army continued to perform these tasks until the Air Force was able to assemble the facilities and resources to assume them.

C. U.S. Navy

U.S. Navy regulations in force throughout WWII directed that all codes and ciphers and signal publications would be produced by the Chief of Naval Operations. To meet the requirements of these regulations, a communications security organization was established under the Chief of Naval Communications to carry out the most important functions:

- a. Research was performed by the cryptographic research section (OP-204D). This section determined cryptographic principles of U.S. Naval cryptographic aids, and produced breadboard models of new machine and devices resulting from its research.

- b. Engineering developments were carried out by the Naval Code and Signal Laboratory. This facility completed engineering on equipment and designs, and overhauled - and

~~SECRET~~

also manufactured in its own shops - a considerable portion of the cryptographic machines and devices used by the Navy.

c. Production of printed cryptodocuments was performed in the Cryptographic Aids Section (OP-204Y) under the Chief of Naval Communications, in the office of the CNO. Field cryptographic reproduction offices, such as the one at Pearl Harbor, reproduced cryptographic aids for their areas from copy furnished by OP-204Y.

d. Compilation of key lists and code vocabularies, and the preparation of wiring diagrams and operating instructions, were also functions of OP-204Y. None of these tasks was performed at field offices.

e. Distribution and accounting of registered cryptographic aids was handled by the Registered Publication Section (OP-204R) in Washington, and by 22 subordinate Issuing Offices located throughout the world.

f. Communications Security Rules were formulated in the COMSEC section (OP-204K). This section supervised the operation of the Navy's communication security activities in Washington and in the field, and also determined through its cryptanalysis and traffic analysis sections when compromise of Navy cryptographic systems had occurred or were likely to occur.

The Bureau of Ships was responsible for the production of cryptographic devices and machines. The Bureau would let commercial contracts for such equipment or assign project orders for their manufacture to the Naval Code and Signal laboratory. Requirements for production were established by the Chief of Naval Communications.

The Navy's Research and Development program, and the allocation of funds to support the program, were submitted to the Research and Development Board for consideration. The Navy cryptologic procurement program, and the allocation of funds to carry it out, were approved by the Munitions Board.

~~SECRET~~

Chapter 2

Interservice Coordination

Part II

APPROACHING A TRANSITIONAL PERIOD

As the military services looked to the post war period, certain considerations indicated a need for much closer collatoration - and perhaps even for a complete merger - of the two existing COMINT Agencies, i.e., the Navy Communications Security Agency (CSA) and the Army Security Agency (ASA). One overriding consideration was that continuity of COMINT and COMSEC operations would have to be preserved in order to maintain readiness for possible future emergencies. The organizations which would result from close collaboration or merger would be directed in a manner which would prevent another Pearl Harbor, and would be trained and equipped to serve the combat forces from the very beginning of any hostilities.

One of the most difficult problems arising out of such a consolidation would be that of fusing the essentially military organization of Navy's CSA with the essentially civilian organization of Army's ASA. A primary purpose of a consolidation would be to conserve and make maximum use of the limited number of personnel who were trained and experienced in COMINT matters. Thus it was most important that any new organization be established along lines that would not only assure retention of the personnel who were employed by CSA and ASA, but also would attract new personnel of the requisite caliber, both civilian and military.

To aid in effecting such a merger, an unofficial working level group was formed. This resulted from an agreement reached in February 1944, between leaders of the Army and the Navy.¹ The group was known as the Army-Navy Communication Intelligence Coordinating Committee (ANCICC). This committee, along with other committees and groups, formulated and viewed various studies and proposals which resulted eventually in the formation of the Armed Forces Security Agency (AFSA).

~~SECRET~~

¹Secret Army-Navy Agreement for the Exchange of Communications Intelligence, signed 4 February 1944. Photostat copy in Wenger files, folder: Army-Navy CI collaboration.

Originating as a purely unofficial, working level group established by agreement between the heads of the two COMINT organizations, ANCICC at first had no formal organization beyond the minimum necessary for its immediate operations.¹ An organizational bulletin in the form of an "official description" of ANCICC, prepared by its Secretariat was approved on 8 November 1944,² and was distributed, along with a roster of subcommittees and a schedule of prospective meetings, to the committee members on 10 November 1944.³ ANCICC itself had the following members:

Deputy Chief, Military Intelligence Service, U.S. Army, Colonel C. W. Clarke.

Commanding Officer, Signal Security Agency, U.S. Army, Colonel W. P. Corderman

¹For its first two meetings, 18 April and 10 May 1944, it took the name Army-Navy Radio Intelligence Coordinating Committee.

²Top Secret Minutes of ANCICC Meeting of 8 November 1944, pp 12-15. AG rec.

³Top Secret. ANCICC General Information - No. 1, 10 November 1944. AG Rec. Assistant Director of Naval Communications (OP-20G), U.S. Navy, Captain J. N. Wenger.

Officer in Charge, Naval Communications Annex, U.S. Navy, Captain P. R. Kinney.

Assistant, Combat Intelligence, COMINCH, U.S. Navy, Captain W. R. Smedberg, III.

Its standing subcommittees consisted of members of the Army's G-2 and Signal Security Agency (SSA); The Navy's Office of Naval Intelligence (ONI); and OP-20G (including NEGAT). Normally, each service supplied at least two members of a subcommittee, with the senior office of the host station for a given meeting acting as chairman. The light original subcommittees were as follows:

Intercept and Direction-Finding Cryptanalysis

Traffic Analysis Research

COMINT Communications Frequency Allocation Coverage

Collateral Information Intelligence and Security

~~SECRET~~

Each subcommittee was expected to meet at least once a month, and to submit to ANCICC a monthly report containing a record of proceedings and a list of policy matters requiring ANCICC's decision. It was expected to establish its own procedures, to make and to implement decisions on specific matters insofar as the individual members possessed authority to commit their respective services, to initiate studies and projects of coordination, and to make recommendations to ANCICC. Each subcommittee could establish working committees

The rule of decision by unanimity applied to all formal action by either ANCICC or any of its subcommittees. In the absence of unanimous agreement, each subcommittee report (majority and minority) was signed by those who favored it, and was forwarded to ANCICC. Whenever ANCICC failed to agree, the matter was referred to the higher authorities of the two services. In brief, ANCICC's administrative organization was devised to facilitate mutually beneficial operations through exchanges of information between agencies deeply engaged in the conduct of war, and wholly through voluntary action.

The status of ANCICC did not change until it was given a more official character after nearly a year of existence. An interservice agreement in the form of a joint memorandum signed by the Army Chief of Staff and the Chief of Naval Operations on 10 March 1945¹ established a new higher-level board, designated as the Army-Navy Communication Intelligence Board (ANCIB) with the following membership:

Assistant Chief of Staff for Combat Intelligence, U.S. Fleet

Director of Naval Communications

Assistant Chief of Staff, G-2, War Department General Staff

Commanding Officer, Signal Security Agency

For security reasons, it was to remain outside the framework of the Joint Chief of Staff's Secretariat, and to report directly to the two signatories, exercising its authority subject to their joint approval. The functions assigned to the Board were to coordinate the plans and operations of the communication intelligence organizations of the Army and the Navy; to formulate joint agreements as to pertinent procedures; and to negotiate and coordinate with other intelligence

~~SECRET~~

organizations. The status of ANCICC was formalized by the authority bestowed on the Board to establish a working committee and principal advisory body composed of representatives of the members of ANCIB. ANCICC's organization, as well as its regulations, procedures and duties were determined by ANCIB. The effect of this action was to give recognition to the previously established working committee as an interservice agency, although in a subordinate role.

The ANCIB structure was formalized in an organizational bulletin of 27 June 1945.¹ It was expected that ANCICC and its standing committees would perform most of the work for coordination, while ANCIB met only "to decide questions of major policy and to consider matters upon which ANCICC cannot reach agreement." Whenever necessary, ANCIB and ANCICC would meet jointly; both groups would use the same secretariat. The rule of unanimity for all decisions remained in effect. ANCICC received "authority to make and implement decisions on all matters within the cognizance of ANCIB, except those involving major policy, which should be referred to ANCIB." The previous membership of ANCICC was changed only by substituting the officer-in-charge, U.S. Naval Supplementary Radio Activity, Washington, for the Officer-in Charge, Naval Communications Annex. Seven out of nine ANCIB meetings in 1945 were joint meetings with ANCICC.¹ Determination that any matter involved major policy apparently rested with ANCICC, which went on working much as it had before the Board's establishment. Its subcommittees remained unchanged except for the amalgamation in the ANCRAD subcommittee of two separate units previously known as subcommittees on cryptanalysis and on Research, and for the change in designation of another subcommittee from "frequency allocation coverage" to "Intercept Coordination." The ANCICC subcommittees are shown in the following reorganization chart.²

~~—SECRET—~~

During the 1945-1949, the Armed Forces paralleled their coordinated effort in COMINT in the area of COMSEC also, to the degree necessary for efficient intra service and combined communications. A Joint Security and Cryptographic Panel of the Joint Communications Electronics Committee attended to COMSEC aspects within that committee's jurisdiction. Joint Army-Navy Publications included a series of communications, instructions, and rules for recognition and identification. Although they were mandatory only for joint communications, some were also applied voluntarily to intra-Service communications, thus broadening the area of uniform practices. One Service, in contracting for and procuring major items of intra-Service cryptographic equipment for its own use occasionally expanded a contract to take care of the needs of the other Service. Cryptographic documents used by both Services were produced by one of them in quantities sufficient for the requirements of both. The Army Security Agency and the Navy each helped other departments and agencies of the United States Government, and of Allied Governments, to obtain cryptographic materials for their use. But each Service had its special operational characteristics which affected its means and methods of communication, and which therefore, created differing COMSEC requirements.

In cryptographic research and development, the Navy insisted on independent action. Considering the degree of its dependence on radio communications at sea, and its highly successful exploitation of COMINT as operational intelligence during World War II, every means of confining knowledge of its cryptographic activities so those who needed to know seemed well justified. The Navy's COMSEC organization was distinct from that engaged in Navy COMINT activities. While the latter was under the Deputy Chief of Naval Communications for Supplemental activities, COMSEC activities were under the Deputy Chief of Naval Communications for Administration. The Navy's cryptographic work was carried on by cryptographics research, cryptographic aids, communications security, and registered publication units. In the Army Security Agency, both types of activity were carried on under one administrative roof.

Besides research and development in cryptography, standard COMSEC activities consisted of the preparation of codes, and ciphers and other cryptographic aids such as key lists.

~~SECRET~~

wiring diagrams, and operating instructions for cipher machines, and their distribution to users. They included continuous monitoring of actual service traffic to discover compromises or weaknesses in a service's own cryptographic systems. Cryptographic devices not only had to be procured and distributed, but also had to be repaired and maintained within a Service's secure system.

Each service conducted COMSEC activities in its own way. ASA had the simple administrative structure but the Navy's older organization probably functioned as effectively. In 1948 ASA had a Research and Development Division and a Security Division, branches of which accomplished all COMSEC activities except procurement. At that time the Navy's units under the Deputy Chief of Naval Communications for Administration had to utilize the Bureau of Ships, an office which was not under the jurisdiction of the Chief of Naval Operations in order to complete the engineering development of promising new cryptographic devices. When mechanisms had been officially approved for use, the Chief of Naval Communications determined the quantities required, and the Bureau of Ships had them manufactured, as projects in the Naval Code and Signal Laboratory or under commercial contracts. In a somewhat similar fashion, ASA went outside the jurisdiction of the Chief of Military Intelligence, within which it normally came, to obtain its cryptographic devices. Their procurement was accomplished by the Army Signal Corps, which incorporated ASA's budget in its own.

The Navy relied on a Cryptographic Aids Section to prepare and produce such materials, while the Army (and Air Force) used the comparable Material Branch of ASA's Security Division. When it came to distribution of such material, however, the Navy utilized its separate Registered Publications System consisting of a section in Washington and 22 issuing offices dispersed around the world. The Army (and Air Force) included this function of distribution among those within the cognizance of the Material Branch.

Determining Army and Air Force procedures and supervising their employment, and monitoring to test the vulnerability of crypto-systems, were done by two parts of ASA's security

~~SECRET~~

~~COMINT~~

division (the Methods and Protective Branches.) In the Navy one unit, the Communication Security Section, carried out both those function.

Eventually, an Air Force cryptologic agency would assume for the independent Department of the Air Force, both the COMSEC and COMINT functions being provided for it by ASA. Coordination of such COMSEC activities, at least to the point of preventing inadvertent damage by one Service to another's COMSEC, was an obvious necessity. How far beyond that point coordination could advantageously go with a highly complex problem.

EO 1.4.(c)
P.L. 86-36

Because ASA's authority extended to COMSEC while CSA's did not, the USCICC's Intelligence and Security Subcommittee had to approach COMSEC problems with less firmness than it applied to those related to COMINT. An Policy, for example, was wholly within the province of USCICC, but a Manipulative Communication Deception Policy could only be treated as a subject for coordination with the separate Communication Security Unit, OP-20-K, also under the Navy's Director of Communications.

Certain legislation respecting the security of COMINT activities concerned USCICC. It's subcommittee on Intelligence and Security was made responsible for liaison in relation to bills for the purpose. The Espionage Act of 1917, the Act of 10 June 1933 (18 Stat. 122), the Federal Communications Act of 1934, and the laws governing the granting of patents for secret cryptographic devices all were vehicles for proposed amendments. The existing laws penalized disclosures with respect to United States or foreign diplomatic codes and ciphers, but not unless the actions were deliberately intended to injure the United States, and applied to military matters. What USCICC desired was a prohibition of disclosure, even though innocent of any intention to damage the United States, of any American Code or cipher, or of the fact that a foreign code or cipher had been "broken," actions which actually did damage the United States. Secret devices for cryptanalysis or cryptography needed the protection not only of patents, but of silence concerning the very nature of the devices. USCICC watched developments in regard to Congressional legislation, and worked out a draft agreement and a draft statement for the use of the Secretary of Defense (*Forrestal*) in 1947 in supporting the security legislation before Congress.¹

26 ~~SECRET~~

~~COMINT~~

~~SECRET~~

Although in 1948 the COMINT agencies of the Armed Services withstood, through USCIB, an attempt to subject them to the Control of the Director of Central Intelligence, and escaped from the threat of a separate FCC FBI COMINT undertaking, they did undergo the first stage of a more successful attack upon the kind of control and coordination which they themselves had nurtured. This third development, which stemmed from the Office of the Secretary of Defense, was supported chiefly by considerations of economy.

THE SITUATION AT THE END OF WORLD WAR II

At the end of hostilities, the Armed Forces possessed two substantial agencies for producing communications intelligence (COMINT) and maintaining communications security (COMSEC). The Army and the Navy had each formed organizations of more than 10,000 persons to accomplish these purposes. Their rosters started shrinking soon after the German surrender, but when the fighting in the Pacific also ended about three months later, they were still large, going concerns. The inevitable post-war readjustments which they faced seemed likely to diminish greatly their ability to furnish communication intelligence of the quality and volume which might yield substantial advantages in peacetime.¹

While the Navy's Communications Support Activity and the Army Security Agency were developing the means of coordinated service effort in cryptanalysis, at the working level some mutual assistance in cryptanalytic research was effected through an informal, interservice committee which originated in mid 1944. Known as the Army-Navy Cryptanalytical Research and Development Committee (ANCRAD), and subsequently to be regarded as a subsidiary of ANCICC,² it then exchanged information concerning work on devices for use in emission identification, direction finding, interception, and cryptanalysis.¹

ANCRAD functioned steadily from 1944 to 1949. This committee was not itself engaged in directing research and development, only in coordinating the efforts of ASA and CSA/W, through cognizance of a growing and impressive array of projects. In an auxiliary role, it compiled a set of classifications and of unclassified code names for the many cryptanalytic devices possessed by the two agencies, and for the foreign cryptographic devices with which they were concerned. It

~~SECRET~~

also prepared and issued a glossary of cryptologic terms and other reference and training aids. Research and development in the field of cryptography, however, remained a matter of separate action in which cooperation was less official and complete.

During the final stage of the negotiations which resulted in the Joint Operating Plan of April 1946, the Acting Chief, ASA's Colone Hayes, proposed that ASA and OP 20-G coordinate their cryptographic research and development. New and important achievements in that field were on the horizon, he noted, and considerations of efficiency would encourage maximum application of the principle of common use of completed devices, and the avoidance of duplicated work in providing them. His proposal called for recommendations by the new committee as to which of the services "should undertake primary responsibility in the conduct of special projects of joint interest." Neither service would be hampered in undertaking whatever its operational requirements dictated, but information would be exchanged when its timeliness might influence the course of development.

The Chief of Naval Communications was prepared to enter into an association with ASA on cryptographic research, development, and procurement matters with one proviso, that either service should remain free to reserve from the other information on any development which that service considered to have only intra-service application. ASA accepted this limitation. A first meeting on an informal basis occurred on 22 April 1946, and by early July of that year an agreement establishing the Army-Navy Crypto-Equipment Coordinating Committee, ANCRECC, had been drafted. Members of the committee and its subcommittees on ciphoney and cifax, on cipher machines, and on procurement, were designated by the Chief of Naval Communications on 19 June 1946, and by the Chief of ASA ten days later.

ANCRECC met irregularly either for general exchanges of information or for the discussion of particular problems, or for a demonstration of equipments under development. It helped to formulate a single U.S. position on such COMSEC problems as the modification of the Combined Cipher Machine. ANCRECC remained on an informal, voluntary basis, partly to avoid a membership too numerous to permit uninhibited deliberations. As a purely advisory body, it

~~SECRET~~

accomplished all that could be achieved by sharing knowledge and judgements to advance the interests of joint communications.

On 5 February 1947, Admiral Nimitz, then Chief of Naval Operations, proposed in a memorandum to General Eisenhower, Chief of Staff, U.S. Army, that the existing informal joint committee to exchange technical information on the research and development of crypto-equipment be formalized through their joint approval.¹ In his memorandum to General Eisenhower entitled "Establishment of the Army Navy Crypto-Equipment Coordinating Committee (ANCRECC); Admiral Nimitz cited the fact that the ANCRECC, a joint committee whose objective was the attainment of closer coordination between the services in the field of crypto-equipment,² had been only informally established and he was now proposing to formalize the committee as it was then constituted. Admiral Nimitz observed that, in his view, the committee had been functioning so effectively that its continuance on a formal basis should be assured.

In his response, General Eisenhower stated that even though the informal exchange of technical information between the services had been of considerable mutual benefit, he believed that it would serve no particular purpose to formalize the existing committee because of its very limited authority vis-a-vis coordination between the services. Rather he felt that the research and development of crypto-equipment should be under the cognizance of the Research and Development Board of the Joint Chiefs of Staff. In this way all three services, Army, Navy, and the newly established USAF, would be participating in a common effort to insure a coordinated effort.

On 23 July 1948 the Army proceeded on this tack and proposed that the research and development of crypto-equipment be placed under the cognizance of the Joint Chiefs of Staff's Research and Development Board.

Initially, the Navy indicated that it did not concur, and proposed instead that the charter of the Joint Security and Cryptographic Panel of the Joint Communications Electronics Committee (JCEC)¹ be broadened to include the making of recommendations regarding the research and development of crypto-equipments. In the end though, the Navy did agree to the Army proposal, following which it was coordinated with and concurred in by the USAF.

~~SECRET~~

Coordination Among Defense and Non-Defense Agencies

On 23 September 1944, the Joint Communications Board¹ reported to the Joint Chiefs of Staff on the findings of an ad hoc committee which had investigated cryptographic security activities of several departments and agencies of the government. The report recommended the establishment within the Joint Chiefs of Staff of a permanent cryptographic security board which would have cognizance over the cryptographic activities of all government agencies and departments.

On 20 June 1945 a provisional committee on the security of communications was established by the Joint Communications Board for the purpose of studying the security of U.S. intra- service and joint communications.² This committee considered the following joint and intra-service aspects of their problem:

- a. Education
- b. Terminology and nomenclature
- c. Physical security
- d. Transmission security
- e. Cryptographic procedures

These collective activities regarding the treatment of communications security played a role in the 3 July 1945 issuance of a confidential, unregistered Presidential Executive Order¹ which established a Cryptographic Security Board consisting of the Secretaries of State, War, and the Navy, and charged it with the function of determining and establishing cryptographic security standards and policies in order to achieve the maximum degree of security in all governmental communications. The Cryptographic Security Board was authorized to establish a cryptographic Security Coordinating Committee and other committees as needed, and was also authorized to regulate communications security activities in all parts of the government except the Federal Bureau of Investigation, to which the terms of the Executive Order did not apply. No department or agency was obliged, however, to release information or yield cryptographic practices if its director concluded that it would be in the national interest to retain ^{sole?} jurisdiction over them.²

~~SECRET~~

References

Secret Army Navy Agreement for the Exchange of Communications Intelligence signed 4 February 1944. Photostat copy in Wenger files, folder: Army-Navy C1 collaboration.

For its first two meetings, 18 April and 10 May 1944, it took the name Army-Navy Radio Intelligence Coordinating Committee.

Top Secret Minutes of ANCICC Meeting of 8 November 1944, pp12-15. AG rec.

Top Secret. ANCICC General Information No. 1, 10 November 1944. AG rec.

Top Secret Memo, General Marshall for Admiral King, 9 March 1945, subj: Army-Navy Communications Intelligence Board- Establishment of; Top Secret memo, Chief of Staff, U.S. Army, COMINCH, U.S. Fleet and CNO, for Dir. of Naval Intelligence, Dir of Naval Communications, C of SG-2, CG SSA, 10 March 1945, subj: Army-Navy Communications Intelligence Board, Establishment of, coy appended to USCIB study (prepared by Captain Wenger) "The Status and Authority of USCIB and USCICC," 7 February 1947. In Wenger files.

Top Secret ANCIB Organizational Bulletin No. 1, 27 June 1945. Folder 334-USCIB and USCICC, History of. NSA Library.

Restricted List of Meetings headed "USCIB chairmen" filed in USCIB 4 file. AG records.

Based on Top Secret ANCIB Organizational Bulletin No. 1, 27 June 1945.

Top Secret papers of ANCICC Intelligence and Security Subcommittee. NSA, Technical Library, History File 37; Top Secret Min. Mtgs of SUCICC (39th), 26 March 1947, (41st) 26 May 1947. Captain E.S.L. Goodwin, Captain Wenger, and Mr. W. F. Friedman were involved in drafting what became known as "P.L. 513."

The condition of the Navy's Supplemental Radio Activities Branch (OP-20-G) is described in Naval I.G. Survey, 13 July 1945, Serial 0001791, para. 39. The Army's situation is described in Army Security Agency Top Secret monograph, the "Achievements of the Signal Security Agency in World War II," 28 February 1946, pg 4 NSALIBDOC

~~SECRET~~

Secret Memo, Captain J.W. Fried, S.C., for W. F. Friedman, ND, NS, Folder 334 -
USCRAD (ancrad) NSA Library.

The Army Navy Cryptanalytical Research and Development Committee (ANCRAD) consisted of Commander J.N. Wenger, Commander H.T. Engstrom; and H.W.C. Norris for the Navy; and Colonel H.G. Hayes, Major Leo Rosen, and Mr. William F. Friedman for the Army.

OP-20Y, Serial 03666P20 5 February 1947.

According to the proposed terms of reference, formalization of the Committee was intended "...to expedite research, development, manufacture, and procurement of crypto- equipment, and to obtain maximum benefit from common effort in this field...and to facilitate the exchange of information between the two services...." Because of the highly classified nature of the activities falling within the cognizance of the committee, membership was very limited. The Army was represented by the Chief, Army Security Agency, and members of his office; the Navy by the Chief of Naval Communications and members of his office and of the Bureau of Ships.

After Congress in 1947 had placed the Joint Chiefs of Staff on a statutory basis, created the Department of the Air Force, and recognized the U.S. Air Force as a third, separate Armed Service, the Joint Communications Board ceased to fit the structure of the national military establishment. As a result, it was replaced in May, 1948, by the Joint Communications - Electronics Committee (JCEC) of the Joint Chiefs of Staff.

Joint Communications Board 174/10/D, 20 June 1945.

Get and quote verbatim

"Study of a Joint Organization for the Security of U.S. Military Communications."

Prepared for the Stone Board. Part B.

~~SECRET~~

CHAPTER 3

Part I. The Elements of Communications Security

Most members of the cryptologic community have a fairly good knowledge of what the term "communications security" means. But just in case there are some who do not, communications security (COMSEC) can best be defined as being the natural and direct defense against communications intelligence (COMINT). Just as communications intelligence has three elements, cryptanalysis, traffic-analysis, and the use of information picked up through normal intelligence channels, so also does communication security have three distinct elements, i.e., cryptologic security - the defense against cryptanalysis; transmission security - the defense against traffic analysis; and physical security - the defense against espionage and other intelligence gathering means. Putting these three defenses together gives a working definition of communication security, which can be stated simply as being "the sum of all of the measures necessary to deny to unauthorized persons the possibility of deriving intelligence from one's own communications." Actually, communication security is the state which results from successfully implementing all these measures, so it can be described as an active thing, i.e., something which is done; and also as an inactive thing, i.e., a condition which is achieved.

The following is a broad summary of how the whole field of communications security was controlled and how it operated during the period after World War II and for the years up to about 1955. In the mid-1950s, major technological advances resulted in major changes in the mechanical and manual aspects of communications security, but certainly not in the philosophical bases of this vital responsibility. It is important to note that during this time communications security measures in the U.S. were applied almost exclusively to communications of the military services and of the State Department.

The elements which comprise communications security are:

Cryptographic Security - This consists of the provision of cryptographic systems which are inherently secure; provision of the rules, regulations, and policies to govern their use; and the execution of proper measures to insure their correct use.

Transmission Security - This is the part of communications security which results from all measures designed and activated to protect transmissions from interception and traffic analysis.

Physical Security - This amounts simply to taking the necessary precautions to ensure physical protection of crypto equipment or material.

Up until the mid-1950s, the process of achieving cryptographic security usually began with a requirement. This could be submitted by one of the military services, or by all services jointly. The requirement stated the need for a secure cryptographic system to fill a particular communications need. It stipulated certain specifications to be met, certain desired characteristics as to speed, reliability, and security, and perhaps others such as size and weight. If the requirement could be met by existing cryptosystems, the proper materials would have been provided and the job was relatively simple. But if it was a new requirement, a newly expressed need which had not arisen before, a different procedure was called for.

a. Requirement, Production, Control. First, a research project would be established. Engineers would devise an equipment which would meet the physical requirements; cryptographic experts would "invent" a cryptographic component which would fit into the geographical limitations imposed upon them, and one which would afford the necessary degree of cryptographic security, one which would resist cryptanalytic attack by other COMINT organizations. When this was completed, the project would usually be turned over to an outside commercial development company. Here the fine points were completed, development models made and tested, and the specifications and designs for mass production established. Following this a production contract was let, the manufacturer tooled up for the job, and the first production models were provided. These were then turned over to the originators of the initial requirement, and they would conduct service tests. As a result of the tests, production modifications were made if necessary, and the

~~SECRET~~

equipments were then produced. Thus, in keeping with the definition of crypto security through the first step, provision of an inherently secure system was completed.

While the production of basic equipment was going ahead at some commercial plant, AFSA/NSA was manufacturing, in its own facilities, the materials that had to be provided with the equipment. As was generally the case, most cryptosystems consisted of a basic, unvariable method of operation, usually a machine and, in addition, certain variable elements. It was these latter variables which were produced by AFSA/NSA. Usually they consisted of cipher rotors, small wheels with electrical circuits through them, which could be placed in a cipher machine in a large number of ways and which performed the actual process of encipherment. These would be accompanied by key lists, printed sheets which told an operator how he was to arrange his variable elements for the message he was to encipher.

The bulk of the manufacture of this type of material was done by the cryptologic agency, with commercial assistance. For example, blank rotor shells were produced outside, but the wiring and all other security features that went into a completed rotor were inserted at AFSA/NSA.

The next step in the birth of a new cipher system had really been going on all the time. Various ways of using the system had been under study and finally a procedure for its use had been decided upon, a procedure which would maintain the inherent security of the system and at the same time be as simple and easy on the operator as was possible. This procedure was then written up and printed as a document which went to each user of the system. Also published were statements of policy on use of the system, physical security regulations that had to be observed in its use, and other general rules governing its employment.

At that point everything was turned over to the services, machines, rotors, keylists, etc. The first set of material was usually especially made for training, and the Services trained their cryptographic technicians in the new system. The operational material was then distributed to the users, an effective date was promulgated, and the new system was put into operation. Once it was in use the services were responsible for seeing that the rules were properly followed. In order to insure that proper action was taken when serious mistakes occurred, a violation reporting

~~SECRET~~

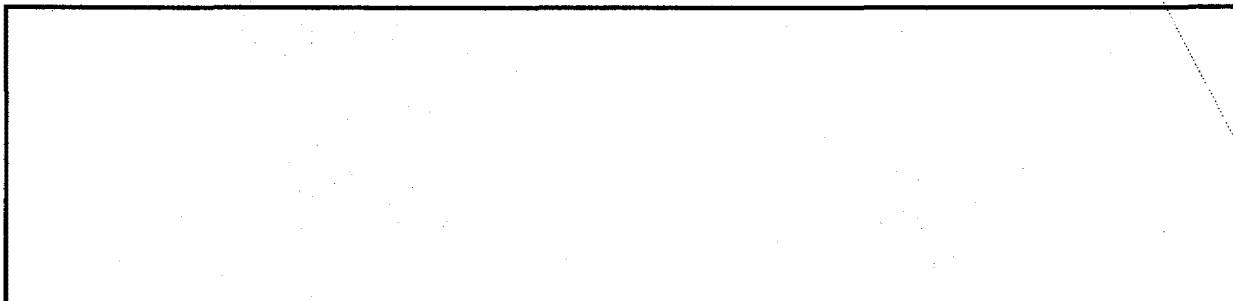
procedure was put into effect. This consisted of a requirement that any command or service element making a mistake in an encrypted message, or learning of a violation of physical security, had to make a report to the proper authorities citing the circumstances. The case was then evaluated in terms of cryptanalytic significance, and the sending organization was informed of the action which had to be taken. In all instances AFSA/NSA was responsible for determining the effect of the violation and for determining what corrective action would be taken in the way of superseding a system, correction a procedural deficiency, or clarifying existing instructions. Other actions to prevent recurrence, improved training, disciplinary action, improved supervision, etc., were purely user (mainly military services) responsibilities.

Closely interwoven in this pattern of control was cryptosecurity's companion element, physical security. Physical security of cryptomaterial breaks down into three main aspects - establishment of safeguards governing the material itself, i.e., how it should be protected in transit and while in use, and what accounting records needed to be maintained on it; safeguards governing protection of the area in which it was used, i.e., what kind of facilities had to be provided, guards, barred windows, limited access, etc.; and safeguarding against personnel defections and carelessness by the establishment of personnel clearance provisions. In all of these AFSA/NSA established the standards considered necessary; they were usually the minimum standards, however, to institute their own more restrictive rules if they so desired.

The transmission security (TRANSEC) element of communication security was and is as critical to the system as was the cryptographic and physical security aspects. Transmission security is best defined as the taking of all measures necessary to protect communications from unauthorized interception, traffic analysis, and initiative deception. There is no absolute defense against interception because almost anything that is transmitted can be intercepted. But there are some means of transmission which can be much more difficult to intercept than others. Therefore, when "measures necessary to protect communications from unauthorized interception" are used, what is really meant is the execution of steps designed to make interception as difficult as possible. Included in these protective measures are:

- 1) the use of specialized radio equipment, special antennas, frequencies, etc.
- 2) protected landlines
- 3) registration of and accounting for, documents and equipment
- 4) specialized transmissions, i.e., infra-red, laser, etc.
- 5) monitoring of friendly communications circuits for security supervision.

EO 1.4.(c)
P.L. 86-36



Transmission security is, then, what is done to prevent loss of intelligence from the external message characteristics by protecting the signal during the act of communications.

New developments in communications techniques and in communications security equipments and procedures started to appear in strength beginning around the mid-1950s. Generally speaking, cipher systems up till then had been of three kinds, manual systems with encryption done entirely by hand; off-line machine systems in which encryption was done mechanically with the result still left to be transmitted; and on-line teletype systems in which encryption took place simultaneously with transmission. We had reached a peak in this latter kind of development by 1954-1955. One new off-line cipher machine had just been given its final service test and was in production, and others were just a few months away. But even those new units, which were basic systems for the next six or seven years, were geared to more-or-less old fashioned concepts of communications.

The first new concept, not new really but certainly in the early-to-mid 1950s just beginning to see the light of day as an actuality, was fully automatic switching equipment at relay centers. Relay installations of that era consisted of a line receiving circuit, a typing reperforator which produced the received message, and a teletype transmitter for each send channel which read the perforations on a tape introduced into it and caused the tape to be transmitted to the

~~SECRET~~

appropriate receiving point or next relay station. The gap between receive reperforator and teletype transmitter was spanned manually. The purpose of the newly introduced equipment was to span it automatically, to transfer messages from receive point to transmit point electrically without any requirement for handling messages physically.

Automatic equipment which was designed and became available in that period was capable of checking incoming channel continuity numbers, recognizing message precedence and routing information, and automatically transmitting messages via cross office circuits to the correct outgoing circuits. The demand for strict communications security complicated all of this, since cryptographic equipment associated with the relay equipment also was required to provide an equal degree of automaticity, and this was quite difficult to achieve. The signals transmitted as switching information, that gave precedence and routing "instructions," had to be in plain, unencrypted form in the switching centers. Therefore, the principle of "link encryption" was adopted. This meant that a message, automatically encrypted at its point of origin, was automatically decrypted, routed to the proper outchannel, and reencrypted at each relay point. The circuits between relay points were in constant use, with an enciphered signal continuously transmitted whether intelligence was being transmitted or not. When a message was entered into the system everything, heading and all, was encrypted. Thus, an almost perfect answer to traffic analysis had been devised. On circuits such as these, it was impossible for interceptors to detect the existence of messages, and the first traffic analysis tool, volume count, disappeared. The other tricks of the trade, routing instructions, precedence information, call signs and the like were equally absent.

But the development problem was by no means licked. There was not an entirely suitable switching equipment, nor did any of the contemplated ones permit, without some basic changes, association with cryptosystems believed to be workable at that time. It was a long while, into the late 1950s before completely secure automatic relay arrangements were in operation.

~~SECRET~~

Part II

B. 1.

B. The augmentation and Management of National COMSEC Resources.

1. The Formation of the Armed Forces Security Agency, AFSA.

While the COMINT agencies tried out a joint operating plan, complete unification of the nation's armed services within a single department of defense was not achieved until the spring of 1947.¹

The National Security Act of 1947² created a National Security Organization of which the major elements were the National Military Establishment, the National Security Council, and the National Security Resources Board. A civilian Secretary of Defense, having an office but not a department, headed the National Military establishment. The Joint Chiefs of Staff, four members with a joint staff were named the principal military advisors to the President and Secretary of Defense. Three departments (Army, Navy, and Air Force) headed by Secretaries without cabinet rank, were established.

The National Security Council was designed to provide the President with advice on the basis of which to integrate domestic, foreign, and military policies. It brought into association for the purpose the President, the Secretary of State, the Secretary of Defense, and his three subordinate secretaries of the Army, Navy, and Air Force, the chairman of the National Security Resources Board and, by presidential designation other heads of executive departments and boards.

Directly under the National Security Council, with the mission of coordinating the intelligence activities of the Federal Government which were concerned with national security, was a Central Intelligence Agency, headed by a Director of Central Intelligence. This Agency was expected to correlate, evaluate, and disseminate national security intelligence, render intelligence services to other agencies and Federal departments, and advise the National Security Council on intelligence matters.

Lastly, the National Security organization included the National Security Resources Board which, like the National Security Council, had direct relationships with the President.

~~SECRET~~

Its mission was to advise the President concerning the coordination of military, industrial, and civilian mobilization, and the base that advice on programs for the most effective use in wartime of manpower and resources.

In September 1947, James Forrestal was installed as the first Secretary of Defense.

Against this background of service unification, those officials responsible for conducting communications intelligence (COMINT) and communications security (COMSEC) operations were considering the ways and means of best coordinating their own efforts. From February to July, 1948, the make up the authorities and the responsibilities of the United States Communications Intelligence Board¹ were being analyzed at length. On 1 July 1948, National Security Council Intelligence Directive (NSCID) No. 9, became the USCIB's new charter. It designated the Board as the National Security Council's agent "the effect the authoritative coordination of communications intelligence for which the Director of Central Intelligence is responsible."² Some members of USCIB undertook a study for the Secretary of Defense to determine the merits of merging the COMINT and COMSEC activities of the Armed Services into a single agency.

On 20 May 1949, Secretary of Defense Johnson, acting under authority given him by the National Security Act of 1947, issued a directive to the Joint Chiefs of Staff. This directive established -- within the National Military Establishment and under the direction and control of the JCS -- a unified cryptologic organization to be known as the Armed Forces Security Agency, or, in shortened form A.F.S.A.'s functions were to be determined by the Joint Chiefs of Staff, and were to be provided by ASA, CSA, and a comparable organization from the Air Force (this eventually turned out to be the Air Force Security Service - AFSS)

Responsibilities for communications security during the period preceeding the formation of AFSA were related to, but separate from, those for COMINT. By a confidential, unregistered Executive Order dated 3 July 1945,¹ the President had established a cryptographic Security Board consisting of the Secretaries of State, War, and Navy, and had charged it with the function of determining and establishing cryptographic security standards and policies in order to achieve the maximum degree of security in all Governmental communications. The cryptographic Security

40-~~SECRET~~

~~SECRET~~

Board was permitted to create a cryptographic Security Coordinating Committee and other committees as needed, and authorized to regulate communications security in all parts of the government except the Federal Bureau of Investigation, to which the terms of the Executive Order did not apply. No department or agency was obliged, however, to release information or yield cryptographic practices if its director concluded that it would be in the national interest to retain them.²

The Committee on the Creation of a Unified Armed Forces Security Agency (The "Stone Board.")

The official separation of the Air Force from the Army on 19 September 1947 involved arrangements by which the Army continued to provide various services to the Air Force, among them the production of strategic COMINT. The Air Force for some of the same reasons which prompted the Army and Navy to retain control of COMINT production within their own chains of command, prepared to establish an Air Force COMINT agency. On 3 June 1948 Headquarters, ASA, established an Air Force Security Group (AFSG) as a unit within its own plans and operations staff. The group was commanded by Major Idris Jones, an officer experienced in both Communications and comint. Working jointly ASA and the USAF Security Group formulated tables of organization, requirements, operating procedures, etc., and on 23 June 1948 the U. S. Air Force Security Group was formally announced to the major commands of the Air Force.

The Department of the Air Force incorporated the AFSG within a new U. S. Air Force Security Service, a major command reporting through the Director of Intelligence, USAF, to the Deputy Chief of Staff for Operations and the Chief of Staff, USAF. Formal establishment occurred on 20 October 1948. At the end of the following January, ASA released to the USAFSS the personnel and property of three radio squadrons, plus some staff members. On 1 February 1948, at Arlington Hall Station, the commander, USAFSS, assumed command.¹

Secretary of Defense Forrestal had sought in the meantime to escape avoidable new casts for cryptologic activities. He planned, with encouragement from Secretary of the Army Kenneth S. Royall, to ascertain the possibility of combining in one unit all existing military COMINT services

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

"at the Washington level" rather than of permitting duplication to expand into triplication. The secretary's objective was to determine how costs for COMINT might be reduced. The annual cost of starting up an Air Force Agency was then estimated to be nearly

On 3 August 1948, a study of the possibility of creating a unified Armed Forces Security Agency was initiated. The study was to be conducted by military officers of the National Military Establishment, but to take account also of the cryptologic interests of other segments of the government.²

The secretary of Defense's directive to the committee on the creation of an Armed Forces Security Agency identified the six members of the committee, only one of whom was engaged in COMINT production, as follows:

Department of the Army

Major General A. R. Bolling, Associate CS, G-2, DA Colonel Harold G. Hayes, Chife, Army Security Agency.

Department of the Navy

Rear Admiral Ear E. Stone, Director of Naval Communications.

Captain W S. Veeder, ONI

Department of the Air Force

Major General C. P. Cabell, Director of Intelligence, A-2, USAF

Brigadere General F. L. Ankenbrandt, Director of Communications, USAF.

While General Bolling was instructed to call the Committee's first meeting, the members were authorized to select their own chairman. As a non-voting personal representative at its sessions, the Secretary of Dfense named his executive assistant, Mr. Robert Blum. The date set for submission of the Committee's report, with recommendations, was 15 November 1948.

Secretary Forrestal's directive grouped a series of topics for study under two major queries:

1. Should there be established a joint or unified Armed Forces Agency fo the production of communications intelligence, and if so, what form should it take?

~~SECRET~~

2. Should there be joint or unified Cryptographic Security Activities of the Army, Navy, and Air Force and, if so, what form should they take?

These queries and topics were meant to be illustrative, not restrictive. The committee was authorized to take up any related problems. It was instructed to take into consideration the interests of the other members of USCIB, the Department of State, and the Central Intelligence Agency, and to consult them, if appropriate, but its province was only that portion of the COMINT and COMSEC activities of the Government which were under the cognizance of the military departments and were therefore a proper subject for action by the Secretary of Defense. The Terms of Reference, in their use of the words "Cryptographic Security," were interpreted by the committee to mean "Communications Security," embracing not only cryptographic but also transmission and physical security.

The first assembly of the Committee was on 25 August 1948, at the Pentagon. At this organization session, the Committee elected Rear Admiral Earl E. Stone as permanent chairman, an action which caused the committee to be known thereafter as "the Stone Board." The committee agreed that each member might designate an alternate, and also that a Working Group should be created to prepare the studies on which the committee itself would subsequently deliberate. The working Group consisted of the following:

Department of the Army Alternate

Member

Colonel Harold G. Hayes Lieutenant Colonel Paul E. Neff

Lieutenant Colonel A.C.

Peterson Lieutenant Colonel Carter L. Clark

Department of the Navy

Captain J.N. Wenger Commander Bernard Roeder

Captain J.S. Harper Captain E.S.L. Goodwin

~~SECRET~~

Department of the Air Force

Colonel R.P. Klocks Lieutenant Colonel H.H. Towler

Lieut.Col. L.C. Sheetz Major J. MorrisonThe Working Group then established two sub groups, one to study COMINT and the other to study COMSEC, and each to prepare draft proposals for the committee's consideration.¹

The Board's second meeting was largely devoted to furnishing guidance for the Working Group by interpreting the Terms of Reference from the Secretary of Defense. At its third session, however, it had before it a preliminary version of a study of communication security which described possible methods by which the Armed Services could conduct unified comsec activities. The various suggestions were discussed inconclusively but the area on which to seek agreement was narrowed by the obvious, general disapproval of certain possibilities.² After the section of the Stone Board's report concerned with COMSEC had been brought to a stage of provisional agreement, it was reserved in order that all recommendations might be consonant with the pending proposals concerning COMINT activities.

The new inter-service agency which this plan envisioned would engaged in both COMINT production and COMSEC operations. A Research and Development Division, a major factor in the overall concept of COMSEC, having a shop and branches specializing in ciphoney and cifax, electronics and electromechanics, would plan new equipment, prepare models, undertake emergency construction, and maintain existing equipment.

The Agency would be headed for a two-year term by a Director, a Flag or General office who would be chosen in turn from each of the three Armed Services. The Director would be the chairman of an Armed Forces Communications Intelligence Advisory Council (AFCIAC) which would consist of the Service representatives already serving on USCIB, and of not more than one additional representative from each service. The AFCIAC was expected to recommend to the Joint Chiefs of Staff policies, operating plans, and doctrines for the production of COMINT and the maintenance of COMSEC.

~~SECRET~~

20 May 1949

MEMORANDUM FOR THE JOINT CHIEFS OF STAFF

SUBJECT: Organization of Cryptologic Activities within the National Military Establishment

1. The attached directive establishes a unified cryptologic organization--the Armed Forces Security Agency--for the conduct of communications intelligence and communications security activities within the National Military Establishment.
2. It is desired that the common activities of AFSA be conducted in not more than two major establishments. Efficiency and economy are to be stressed.
3. Responsibilities of the Joint Chiefs of Staff are as indicated in the attached directive.

/s/ Louis Johnson

Mission of the Director, AFSA Acquisition of New Functions

The mission of the Director of AFSA, DIRAFSA, would apply not only to COMINT but to military COMSEC also. He was expected normally to prepare, produce, store, account for, and deliver crypto-material for distribution to the Armed Forces. He was also to formulate policies and publish instructions.

On 20 May 1948, Secretary of Defense Louis Johnson sent a covering memorandum¹ to the Joint Chiefs of Staff, with copies to the Service secretaries, which contained a directive describing the establishment of a unified cryptologic organization--the Armed Forces Security Agency. This Agency was to conduct the communications intelligence and communications security activities within the National Military Establishment. Secretary Johnson expressed the desire that the common activities of AFSA be carried out in not more than two major establishments. In this he had in mind ASA's facility at Arlington Hall and CSA's resources at Nebraska Avenue.

The Directive also defined the responsibilities the Joint Chiefs of Staff vis-a-vis the new AFSA.

45 ~~SECRET~~

~~SECRET~~

The mission of the Director of AFSA, DIRAFSA, would apply not only to COMINT but to military COMSEC also. He was expected normally to prepare, produce, store, account for, and deliver crypto-material for distribution to the Armed Forces. He was also to formulate policies and publish instructions necessary for their use, handling, maintenance, and protection. In formulating COMSEC policies, he was expected to deal with its three major elements, cryptographic security, transmission security, and the physical security of cryptologic material, and with the related matters of communications cover and deception, or "cryptologic countermeasures" of any sort. His responsibilities included liaison with other appropriate departments and agencies for the purpose of coordinating cryptologic equipment and procedures, and providing technical supervision of all military COMSEC activities. None of his COMSEC responsibilities came within the jurisdiction of USCIB.

For units of the Armed Forces, AFSA was to establish a method of providing special items of crypt-equipment whenever the standard distribution lists did not provide for them. AFSA was made responsible for preparing and executing coordinated programs of research and development of cryptologic equipment approved by the Research and Development Board of the Department of Defense. With the approval of the new Munitions Board, its responsibility for procuring cryptologic equipment would parallel that for research and development. AFSA was expected to issue technical publications pertaining to its work, to conduct training to meet the standards which it established, and to provide specialized training designed to meet individual Army, Navy, and Air Force needs.

LOCATION OF AFSA

The Director was asked to prepare a paper for forwarding to the Joint Chiefs of Staff indicating two possible plans for the newly formed AFSA organization. The first plan would assume that the two Washington area plants, Arlington Hall and the Navy Communications station at Nebraska Avenue, in Northwest Washington, D.C., were each operated on an integrated basis; the second, that all COMINT activities would be consolidated in one plant and all COMSEC activities in the other. The Director's paper recommended the second plan.

~~SECRET~~

Since Arlington Hall Station could provide 420,000 square feet of operational floor space, and the U.S. Navy Communication Station could furnish 245,000 square feet, the total area available was approximately the total area required for all Washington activities.

AFCIAC accepted the argument in favor of consolidating at one station almost all of the COMINT operations and related research and development, and, at the other site, almost all COMSEC operations with related research and development.

AFSA's first Director assumed office on 15 July 1949 and received a directive from the Joint Chiefs of Staff on 1 September. On the same day, AFSAC obtained its charter. The nucleus of planners and organizers grew and, by a succession of steps taken or planned prepared for the approval of the JCS the outlines of the new Agency's composition, physical location, and headquarters organization.¹ On 1 October 1949 DIRAFSA officially assumed operational control. Two striking features deserve emphasis: the Military Services were establishing an organization through which their production of COMINT would be under unified control, and they were linking the cryptologic agencies of all three Services with reference not only to COMINT production but to COMSEC activities as well.

B. Formation of the Office of Communications Security, AFSA-04.

While fundamental planning defined AFSA's position in the Department of Defense and the relationships to the Armed Services, simultaneous, detailed planning was determining AFSA's internal structure. The first Director depended heavily upon the advice and assistance of key individuals who had been close to the cryptologic activities of the Services during his tour as Chief of Naval Communications. In matters of organization, distribution of functions, selection of personnel for specific key positions, and the relations to be developed between AFSA and the service cryptologic agencies, he relied in particular on Captain J.N. Wenger, USN, who had been his chief subordinate in COMINT matters for several years.

Each Armed Service furnished one Deputy Director soon after Admiral Stone took office in July. Captain J.N. Wenger, USN; Colonel S.P. Collins, USA; and Colonel Roy H. Lynn, USAF, became the official Steering Group, and they served in that capacity until AFSA's organization was

~~SECRET~~

firmly established. Each Deputy Director was given particular functions, with one of his main functions being that of liaison between AFSA and his Service, as the Director preferred. The division of functions prescribed on 29 July 1949 was as follows:¹

Army Deputy Navy Deputy Air Force Deputy

Colonel Collins Captain Wenger Colonel Lynn

Army Liaison Navy Liaison Air Force Liaison
COMSEC Operations-COMINT Administration
Research and CJO Functions Staff Coordination
Development Communications

The pattern of action intended to bring about AFSA's full functioning was sketched in the first organizational memorandum, issued on 22 July 1949. There were to be successively (1) a period of study and planning, (2) a period for the implementation of this plan, in the course of which its merits and defects would become apparent, and (3) a period in which the permanent organization would be established. A Steering Group, besides supervising the work of other groups, was expected to develop an organization plan for AFSA's staff. Four monitor groups were given functional areas of responsibility as follows: Communications Intelligence (COMINT); Communications Security (COMSEC); Research and Development, and Administration. Each of these four groups consisted of one representative from each Service with suitable qualifications. The Monitor Groups were authorized to subdivide the problems in their areas of responsibility, and to parcel out special study and planning tasks to others, while adopting procedures resulting in final, inclusive reports not later than 15 August 1949.

The Communications Security Monitor Group was composed of Dr. A. Sinkov, ASA Chairman; Captain M. R. Gerin, USN; Captain H.O. Hansen, USN; and Lieutenant Colonel J.L. Weeks, USAF. The group succeeded in drawing up a plan for the consolidation of Service COMSEC activities, disagreeing only on the question of operational control of security monitoring units. It was unanimously agreed that the new AFSA office of Communications Security should assume responsibility for planning and policies in the field of COMSEC; for production of all crypto-material for the Armed Forces; for engineering and development of crypto-equipment; for

~~SECRET~~

cryptanalysis and evaluation; for traffic analysis and evaluation; and for procurement of crypto equipment. The Services were to retain responsibility for determination of intra service allowances; distribution and accounting; maintenance; physical security; budgeting; and training (crypto-operators and maintenance personnel). Service testing of crypto-equipment was to be performed by the Services with AFSA providing technical assistance and guidance. The office was to be divided into three divisions, i.e., Crypto Engineering, Documents, and Analysis and Evaluation, with administrative and technical staffs, and a Distribution and Accounting Branch below the division level, responsible directly to the head of the office.

The background of the organization of the office of COMSEC was formed by the provisions relating to COMSEC in the JCS 2010 directives and by the report of the COMSEC Monitor Group. JCS 2010 assigned to AFSA served specific responsibilities in the COMSEC field, such as formulation of policies, production of cryptographic material for the Services, evaluation of crypto-security violations, and technical supervision of Service communication security activities.¹ An amendment to JCS 2010² assigned to the residual Service cryptologic organizations the responsibility for "security monitoring of intra-service circuits."

On 25 August 1949 the Director, AFSA, submitted to AFCIAC a Progress Report describing, in very general terms, the actions thus far taken to organize AFSA, and the principles on which this organization was proceeding. He reported that he had assigned certain specific functional supervisory duties to each of the three Deputy Directors. Responsibility for supervision of COMSEC had been given to the Army Deputy, Colonel Collins. The Director also informed AFCIAC that it had been decided to consolidate all COMSEC activities at the Naval Communications Station as far as possible. This was in accord with the recommendations of the COMSEC Monitor Group.

The first draft of the AFSA organizational manual, which was ready on 26 August, followed the recommendations of the Monitor Group in outlining the organization of the Office of Security. The responsibilities assigned to this Office, and to its subdivisions, were, in general, those of establishment of COMSEC policies; production of crypto-material for the Services,

~~SECRET~~

together with necessary technical instructions; evaluation of violations of security; determining compromises; and formulating policies for communications cover and deception. In addition, the Office of Security was to exercise "operational control of AFSA communication security facilities, units, and military personnel, and operational and administrative control of all civilian personnel of AFSA engaged in communication security duties." It was also responsible for "technical supervision of all communication security activities of the Armed Forces." The organizational structure of the Office followed rather closely the Monitor Group's recommendations, i.e., the office was to have a Technical Staff, three Divisions (Analysis and Evaluation) Documents, and crypto-engineering), and a Distribution and Accounting Branch, below the Division level but not part of any Division.

Details of the division of functions between AFSA and the Services were worked out shortly afterwards, in conferences between DIRAFSA and Service representatives. On the question of COMSEC, it was decided that the Navy should retain its security monitoring service, the Naval Computing Machine laboratory at St. Paul, cryptographic repair and maintenance facilities, cryptologic training schools, and the Registered Publications Section. Twelve men were transferred to AFSA from the Navy's analysis and evaluation of cryptosystems branch and an equal number were to remain under Navy control to perform monitoring functions and other miscellaneous duties. Cryptographic maintenance was to remain a function of the Services, with AFSA exercising a coordinating role. For the time being, Navy would retain the Naval Code and Signal Laboratory which would continue under the management and technical control of the Bureau of Ships. The Bureau also continued its contractual authority until this also could be assumed by AFSA.

Arrangements with the Army were made early in September. The understanding reached at this time was amended at another conference held on 14 October, and was then formalized in a written document¹ dated 22 December 1949. According to this agreement, ASA was to continue to be responsible for communication security within the Army, through such tasks as issuance of crypto-material to Army users, cryptographic maintenance and repair, enforcement of AFSA's

~~SECRET~~

directives on security, etc. AFSA was to be responsible for preparing crypto material for Army use, declaring cryptographic compromises, establishing cryptographic procedures, and conducting cryptanalytic studies for security evaluation. No mention was made of the operation of security monitoring units.

A list of proposed appointments to supervisory positions of the sub-divisions of AFSA was promulgated on 7 September 1949. This list provided for the appointment of Captain M. R. Gerin, USN, as Acting Chief of the Office of Communication Security, AFSA-04, with Dr. A. Sinkov as the Technical Director. The list of division chiefs indicates that there were five divisions provided for, instead of only three, as had been shown in the draft of the Organizational Manual. In addition to the three divisions noted in the latter, there was to be a Distribution and Accounting Branch and a Security Coordinating Division (which had been deleted from the draft manual.¹)

On 23 September 1949, the Director, AFSA, notified ASA and the Chief of Naval Communications that he would assume "operational control of all elements of AFSA at 0001 on 1 October." Appended to this announcement were lists of the units and facilities which would pass under AFSA's control at this time. Those to be taken over from ASA included the Security Division of ASA Headquarters, less the elements required for ASA residual cryptologic functions. Similarly, the Navy was informed that AFSA would take over the Communications Security Section (less elements required for residual Navy functions), the Cryptographic Aids section, and the inactive Cryptographic Reproduction Unit at Pearl Harbor.²

Assimilation of these activities into AFSA, and of the Naval Code and Signal Laboratory as well, had already been approved by AFSCIAC on 8 September. This AFSCIAC decision, finalized on 23 September, was embodied in JCS 2010/10, approved by JCS on 25 October, at which time the decision to Concentrate COMSEC activities at the Naval Communications Station (also approved by AFSCIAC) was also approved as JCS 2010/11.¹

Since AFSA at this time existed largely on paper, it would be necessary, for the time being, for the Director to exercise control over the assimilated units through the existing command channels of ASA Headquarters and of CSA/Washington until the physical consolidation

~~SECRET~~

of these facilities had progressed sufficiently to render this indirect method unnecessary. This fact was pointed out in a memorandum² from OP 202, Captain Holtwick, to the OP 202 staff and the officer-in charge, CSA/W, dated 30 September 1949. The memorandum listed the specific units of OP-202 over which AFSA would assume control on 1 October. Those slated for absorption into AFSA-04, the Office of Communication Security, were OP-202Y, the Cryptographic Aids (or Cryptographic Production) Section, OP-202K2, the Statistics division of OP-202K; OP-202K4, the Cryptanalysis Division; and OP 202K7B, the Cryptographic Monitoring subdivision.

In accordance with the plan, DIRAFSA announced on 1 October, that he was assuming operational control of the Service cryptologic facilities.¹ A fairly complete description of how this affected at least one of the Navy units concerned (OP-202K) was given in a directive² from OP-202, dated 1 November 1949, announcing the formation of AFSA. According to this directive, "all U.S. Navy Communication Security Activities will continue to exist as part of the Navy and to be under the same military command and coordination control as in the past." However, "the OP-202K cryptologic evaluations (cryptanalysis and evaluation of compromises) and statistical functions, and part of the crypto-monitoring functions, are to be transferred to AFSA, together with the personnel engaged primarily in those functions. OP-202K, with the remaining personnel, will continue as the Communications Security Section...to discharge intra-Navy COMSEC responsibilities and maintain liaison with AFSA for communication security responsibilities."¹ Operational control of the Cryptologic Evaluation, Statistics, and crypto-monitoring functions, assumed by AFSA on 1 October would be exercised "through the existing channels."² For the time being, OP-202K would retain operational control of its field activities. "However, it is possible that AFSA may when time does not permit working through 202K, make direct requests to Communications Security Activities for circuit coverage or informational data concerning suspected compromises. Such requests will be complied with."³ Presumably, similar arrangements existed with the corresponding Army activities.

On 15 December 1949, DIRAFSA assumed direct control of those units which he had previously controlled through existing command channels. Consequently, effective the same date,

~~SECRET~~

the office of the Officer-in-Charge, Communications Supplementary Activity, Washington, and of the heads of the units of OP 202 and CSA/W which had passed to AFSA, were abolished. Remaining sections of CSA/W were made a part of the Naval Communication Station organization.¹

Almost simultaneously with this step, DIRAFSA completed the process of taking over the Naval Code and Signal Laboratory, which had remained under Navy control for the time being. Transfer of this activity was a rather complicated process. On 21 September, DIRAFSA requested the Bureau of Ships to take action to have civilian personnel of NCSL placed in excepted positions (Schedule B), for security considerations; this involved transfer of the existing personnel ceiling of 176 to the Navy Communication Station for reappointment of personnel under Schedule B.² This was done on 27 September; the Bureau still retained technical and management control over the Laboratory, but it was agreed that DIRAFSA directives on cryptologic work would, with the concurrence of CNO, be accepted for action.¹ On 9 November, DIRAFSA requested BuShips to have NCSL disestablished by 10 December, or as soon thereafter as possible, transferring all materials and supplies to AFSA, and personnel allowances, projects, and funds to the Naval Communication Station.² Consequently, the laboratory was disestablished, effective 10 December.³ Transfer of the projects to Naval Communication Station, and of material and equipment to AFSA, was done on 14 and 16 December 1949, respectively.¹ However, the transfer of materials required some months, and was not completed before the following summer.²

The organization of the AFSA Office of Security was completed by the issuance of the final draft of the Organization Manual, on 24 March 1950. According to the manual, the activities of the Office were to be conducted in two staff sections and four divisions. The Chief of the Office, in addition to exercising control over the Office, advising DIRAFSA on COMSEC matters, and the like, was to exercise "operational control over such service communications security activities as may be allocated to the operational control of AFSA." The two staffs were 04A3, the Management Staff, and 04A4, the Technical Planning Staff. The latter was charged with preparing the technical plans necessary in connection with the production of crypto-material, and with guidance

~~SECRET~~

of the AFSA cryptographic research and development program, including, in this connection, service testing of new cryptoequipment. The Analysis and Evaluation Division (AFSA- 41) dealt with maintenance of cryptographic security through proper use of cryptosystems, including "examination of encrypted traffic of the Armed Forces for violations of cryptosecurity." For the latter purposes, it was to make arrangements through the Services to obtain traffic for examination. It prescribed operating procedures, based on cryptanalytic studies; evaluated all existing and proposed cryptosystems and devices; established procedures for reporting violations and possible compromises; established policies for uniform service enforcement of transmission security rules; initiated requests to the Services for special security monitoring missions; directing "such surveillance activities of the Armed Forces as are placed under the operational control of AFSA;" and prepared policies for communications cover and deception. Production of cryptographic equipment for the Armed Forces, and related engineering functions, were done by AFSA- 42, the *Crypto-Engineering Division*. The Documents Division, AFSA 43, produced cryptographic documents for use by the Armed Forces. AFSA-44, the Distribution and Accounting Division, was "responsible for the bulk distribution and accounting of all AFSA produced cryptomaterial to the Armed Forces, "also to other governmental agencies and to certain allied governments."

Five diagrams of the organization of AFSA-04, the Office of Communications Security, and mission and function statements to branch level, follow.

~~SECRET~~

Footnotes

The following sources concerning unification of the Armed Forces are worth noting: Walter Millis, ed., *The Forrestal Diaries* (N.Y. 1951), pp 59, and following; Elias Huzar, "Notes on the Unifications Controversy" in *Public Administration Reviews*, VI, No. 4 (Autumn, 1946), pp 297-314; Task Force Report on *National Security Organization*, prepared for the Commission on Organization of the Executive Branch of the Government (as Appendix G), and submitted to Mr. Herbert Hoover by Mr. F. Eberstadt, Chairman of the Committee on National Security Organization, 15 November 1948 (Washington, GPO, 1949).

Public Law 253, 80th Congress.

The Board consisted of representatives from the Departments of State, Army, Navy, and Air Force, and from the Central Intelligence Agency.

NSCID No. 9, Chapter .

President Harry S. Truman's order of 3 July 1945, "Cryptographic Security with Respect to Certain Communications of the Government."

Information derived from a
Study of Joint Organization for the Security of U.S. Military Communications, prepared for the "Stone Board" and included within Part B of its report, and from Communications Division, U.S. Navy, Top Secret Order No. 15-48, 8 September 1948.

History of the USAFSS, I, 1-9, Secret. Annual Report, ASA Staff, FY-48, 1, 5. Top Secret

Memos for the Secretary of Defense from Mr. Robert Blum, Executive Assistant, dated 1 July 1948 and 28 July 1949, and from Army Secretary Royale, dated 24 July 1948, subject: Unified Armed Forces Security Agency.

Memo for Chief, Unification Control Office, DC/S, from Director of Intelligence, GSUSA, dated 23 July 1948.

Memo for the Secretary of Defense from Robert Blum, dated 17 August 1948, Top Secret.

Memo for the Secretaries of the Army, Navy and Air Force from the Secretary of Defense, dated 19

55-~~SECRET~~

~~SECRET~~

August 1948, Subject: Terms of Reference for the Committee on the Creations of a Unified Armed Forces Security Agency.

Minutes of the first meeting, 25 August 1948, and of the second meeting, 3 September 1948, of the Committee on the Creation of a Unified Armed Forces Security Agency. Top Secret (In Sec/Def files.)

Minutes of the third meeting, 1 October 1948; of the Committee for the Creation of a Unified Armed Forces Security Agency. Top Secret. Ibid.

Memorandum for the Joint Chiefs of Staff. Subject: Organization of Cryptologic Activities within the National Military Establishment, dated 20 May 1949, plus attachment: *Directive-Armed Forces Security Agency (AFSA)*.

JCS 2010/10 and JCS 2010/11, dated 30 September 1949. Top Secret.

AFSA Organization Memorandum No. 3, 29 July 1949, Subject: AFSA Headquarters.

JCS 2010

JCS 2010/G, 28 July 1949.

Top Secret Memorandum for the Record, Subject: Discussions Concerning the Proposed Residual Army Cryptologic Organization, CSGAS-23, 6 September 1949, (filed w/minutes of AFSA Staff Meetings; SECRET Memorandum from ASA (CSGAS-23) to DIRAFSA, 22 December 1949, Subject: Interrelationship of Armed Forces Security Agency and Army Security Agency Functions (folder "AFSA-Service Agreements," Tab 11, in Wenger files in Historian's office).

AFSA Organizational Memorandum No. 8, 7 September 1949.

Top Secret Memorandum from Director, AFSA, to Chief, ASA Serial 00016, 23 September 1949; Top Secret memorandum from Director AFSA, to Chief of Naval Operations (CNC00P20), Serial 00017, 23 September 1949. (Both in AFSA Organizational folder - file 771.)

Minutes of Fourth Meeting of AFCIAC, 8 September 1949, and of Fifth Meeting, 23 September 1949; Top Secret JCS 2010/10, 30 September 1949, and Decision on JCS 2010/10 25 October 1949; Top Secret, JCS 201-11, 30 September 1949, and decision on JCS 2010/11, 25 October 1949.

~~SECRET~~

Confidential Memorandum for OP 202 Staff and Officer in Charge, CSA/W, from Captain J. S. Holtwick, OP-202, Serial 02764P20, 30 September 1949 (in AFSA Organization folder file 771). See chart of organization of Communication Security Section (there designated OP0204), dated 1 July 1949, enclosed as Tab 10a in Top Secret Folder No. 3, Organizations of U.S. Navy Cryptologic Activities as of 1 July 1949, Encl. B, CNC Serial 000192P20.

AFSA Order No. 1-49, 1 October 1949. (AFSA Organization folder.)

Letter serial 001013P20, 1 November 1949, from Chief of Naval Communications (OP-202), Captain J.S. Holtwick Jr., to all U.S. Navy Communication Security Activities, Subject: Armed Forces Security Agency; information concerning. (AFSA Organization folder.)

Ibid.

Ibid.

Ibid.

Supplementary Branch Order No. 2-49, 15 December 1949, Subject: Communications Supplementary Activity, Washington; de-activation of. (AFSA Organization folder.)

Letter serial 09, 21 September 1949, from DIRAFSA to Chief of the Bureau of Ships, Subject: Assumption of Operational Control of Cryptologic Activities. Rear Admiral Stone day file.

BuShips serial No. 852-742 to DIRAFSA, 21 October 1949, Subject: U.S. Naval Code and Signed Laboratory, status of. (In folder CSA and NCSL, St. Paul. NSA AG file 771.) Confidential.

Letter serial No. 040, 9 November 1949, from DIRAFSA to Chief of the Bureau of Ships, Subject: U.S. Naval Code and Signal Laboratory, Request for disestablishment of.

BuShips letter Code 740, C-NP(67) A4(743), 1 December 1949 to Assistant Secretary of the Navy, Subject: U.S. Naval Code and Signal Laboratory, Request for disestablishment of, SECNAV letter serial No. 446P24, 6 December 1949.

BuShips letter serial No. 852-939, 14 December 1949, to Commanding Officer, U.S. Navy Communication Station, Subject: U.S. Naval Code and Signal Laboratory, Disestablishment of.

~~SECRET~~

BuShips letter Serial No. 852-949, to Superintendent, U.S. Naval Gun Factory, Washington,
Subject: U.S. Naval Code and Signal Laboratory, Transfer of Equipment and Supplies.

Memorandum for Rear Admiral G. G. Stone, USN, Subject: Disestablishment of the Naval
Code and Signal Laboratory, Actions awaiting completion, 31 July 1950, from NCSL
Disestablishment office, Commander D. W. Seiler, USN. Letter 42 A4-2(1) 078, 3 August 1950,
from Commandant, Potomac River Naval Command to Commanding Officer, Naval
Communication Station, Subject: Disestablishment of NCSL; authority to assume custody of
material in connection therewith.

Armed Forces Security Agency Organizational Manual, 24 March 1950.

~~SECRET~~

OFFICE OF COMMUNICATION SECURITY, AFSA-04

- 04 Chief, Captain H. O. Hansen, USN
- 04A Assistant Chief, Lieutenant Colonel G. V. Johnson, USA
- 04T Technical Director, Dr. A. Sinkov
- 04T1 Assistant Technical Director, Mr. H. L. Clark
- 41 Chief, Analysis and Evaluation Division, Mr. Frank Austin
- 42 Chief, Crypto engineering Division, Mr. Kenneth Kuhn
- 43 Chief, Documents Division, Commander, G. M. Grening

OFFICE OF COMMUNICATION SECURITY, AFSA-04

A. Responsibilities

Responsible for the performance of all COMSEC functions under the cognizance of AFSA.

B. Organization

AFSA-04	Office of the Chief
AFSA-401	Administrative Group
AFSA-402	Planning Group
AFSA-40	Management Group
AFSA-41	Analysis and Evaluation Division
AFSA-42	Crypto-Engineering Division
AFSA-43	Crypto-Aids Division

C. Functions

AFSA-04 - Office of the Chief

1. Exercises control over the subordinate echelons of the Office of Communication Security in the discharge of its assigned responsibilities.
2. Advises and collaborates with all elements of AFSA as required.
3. Insures provision of such technical support as is required of AFSA by the Armed Forces and appropriate government agencies in their conduct of COMSEC activities.

~~SECRET~~

4. Exercises operational control over such Service COMSEC activities as may be allocated to the operational control of AFSA.

5. Insures compliance with applicable security directives, and establishes such additional security safeguards, as may be necessary, within the Office of Communications Security.

6. Provides technical support to Combined and NATO COMSEC activities as directed.

7. Provides members or observers on panels and working groups.

ADMINISTRATIVE GROUP, AFSA-401

1. Coordinates and supervises the application of all administrative and training policies, regulations, and procedures within the Office of Communication Security.

2. Coordinates the training within AFSA-04 of Service personnel attached to AFSA for COMSEC training.

3. Prepares specific job requirements for procurement of AFSA-04 military and civilian personnel.

4. Translates bulk allotments of military and civilian personnel into AFSA-04 Tables of Distribution.

5. Supervises internal security activities of AFSA-04.

6. Within Office of Communication Security:

- a. Administers intra-Office supply procedure.
- b. Insures correct preparation of correspondence.
- c. Provides mail and central file service.
- d. Coordinates historical activities.

7. Administers Top Secret Control for the Office of Communication Security.

PLANNING GROUP, AFSA-402

Performs a coordination function both within the Office of Communication Security and with the Armed Forces outside the Agency. Coordinates technical and operational planning for the Office of Communication Security. Recommends fiscal policies and budget objectives required for

~~SECRET~~

effective operation of Office of Communication Security. Performs long range planning for mobilization. Maintains technical liaison with the Services and prepares a comprehensive long range program for each COMSEC equipment from the time the requirement for a crypto-equipment is first expressed until the equipment is placed into use. Performs special planning in relation to NATO and UKUSA agreements. Advises on COMSEC objectives for inclusion in AFSA plans and, as required, supplies information on or prepares COMSEC portions of these plans.

LONG-RANGE PLANS SECTION, AFSA-402B

1. Prepares statement of the Office of Communication Security program for each Fiscal Year based upon JCS plans for the FY, related plans of the Services, status of research and development program, requirements of the Services, related plans of AFSA, and continuation of authorized "in process" plans.
2. Prepares broad outline of the Office of Communication Security production potential. Coordinates plan with Plans and Policy Division (12) and the Comptroller (OFF).
3. Prepares the Office of Communication Security budget and personnel requirements for FY.
4. Prepares the Office of Communication Security funding program in conjunction with the Comptroller (OFF), the Office of Communication Security staff groups and operating divisions.
5. Recommends fiscal policies and budget assumptions required for effective operation of the Office of Communication Security.
6. Prepares and initiates procurement program for crypto- equipment for FY based upon estimated requirements from Services.
 - a. Initiates action on procurement programs and consolidates Service requisitions and AFSA requirements.
 - b. Maintains liaison with Logistics Division and the Comptroller on bids and contractual and obligating actions.
 - c. Keeps up-to-date on prices, changes in prices, and estimated dates of availability.

~~SECRET~~

7. Prepares mobilization plan for the Office of Communication Security in conjunction with the Office of Communication Security staff groups and operating divisions.

EQUIPMENT PROGRAMS SECTION, AFSA-402C

1. Maintains contact with Services for AFSA on matters relating to communications security equipment under development and procurement.

2. Prepares AFSA communication security research and development program.

3. Prepares long-range program for each communication security equipment, covering from the time the need for an equipment is first expressed as a military characteristic until the equipment is placed into use.

a. Coordinates AFSA's actions on military characteristics and prepares answer to JCEC.

b. Acts to establish R&D projects in AFSA by initiating AFSA/T action. Positions project in program. Prepares AFSA project sheet.

c. Prepares and maintains long-range time schedule covering development, test, and procurement.

d. Maintains detailed liaison with the Office of Research and Development, Office of Communication Security divisions, and Services.

e. Arranges for tests of equipment by Services and for AFSA's participation therein.

f. Furnishes to Logistics Division specifications and drawings for the procurement of COMSEC equipment.

g. Determines when a newly developed COMSEC equipment is ready for procurement.

h. Maintains close coordination check with Office of Communication Security operating divisions on all Office of Communication Security activities related to new equipment.

i. Prepares and maintains detailed time schedule for bringing all elements of a new equipment to completion.

62-~~SECRET~~

~~SECRET~~

j. Establishes Office of Communication Security priorities for Research and Development projects for Communication Security Equipment.

4. Keeps abreast of trends and technical advances in the communication field in order to relate and integrate security equipment to proper communication equipment.

5. Determines by liaison with Service Cryptologic Agencies the type of technical information required by them for conduct of their responsibilities.

PRODUCTION PROGRAMS SECTION, AFSA-402D

1. Gathers long-range quantity requirements for cryptomaterials and equipments periodically from the Services, offices of AFSA, and non-military government agencies. Disseminates information concerning over-all work load to divisions for use in estimating needs and capabilities.

2. Translates the production objective for the year into general monthly production objectives for each major type of material. Phases program build-up or cut-back according to production potential desired at end of Fiscal Year.

3. Determines general type and quantity of cryptomaterials and equipment to be produced for war reserve.

4. Summarizes data supplied by the Services on the rate of the use of cryptomaterial for comparison with production rates and determination of trends.

5. Monitors production activities through close and continuous contact with production units.

6. Recommends areas where simplification studies would be useful and where changes should be made in work measurement schedule.

GENERAL SYSTEMS PLANNING SECTION, AFSA-402E

1. In coordination with each Service and Office of Communication Security operating divisions, determines characteristics and organization (cryptonets, cryptochannels) of cryptosystems which will be brought into use by the introduction of new crypto-equipment. Recommends programs for phased introduction of systems involving new crypto-equipments.

~~SECRET~~

2. For non machine cryptosystems and tactical cryptomaterial involving extensive usage and high volume production, investigates Service need and, in conjunction with operating divisions, initiates plans relating to organization and supply of the material.

3. Performs special planning relating to Combined US UK and NATO communication security materials and operating with particular emphasis upon organization, supply, and use of cryptosystems. Follows through on all Combined and NATO agreement, including the special UKUSA conference, to assure fulfillment of agreements.

4. Performs short term operational planning projects which do not fall into activities of any other Planning Group section.

MANAGEMENT GROUP, AFSA-403

Establishes and maintains programs for realistic and effective business management of the Office of Communications Security with emphasis upon methods, cost, and utilization of resources in order that the Office of Communication Security may effectively meet requirements of the U.S. Armed Forces, other U.S. Government Agencies, and Combined and NATO organizations. Represents the Chief, Office of Communication Security, on management matters. Conducts operations through the Statistical and Cost Control Section and the Operations Management Sections.

STATISTICAL AND COST CONTROL SECTION, AFSA-403B

1. Establishes and reviews stock control and supply procedures required for efficient conduct of the Office of Communication Security operations.

2. Devises and administers a cost accounting system within the Office of Communication Security.

3. Establishes and maintains fiscal records of the Office of Communication Security. Conducts audits of internal Office of Communication Security records.

4. Obtains, summarizes, and publishes production and cost data of all operating divisions.

64 ~~SECRET~~

~~SECRET~~

5. Consolidates periodic progress reports, monthly operational summaries, quarterly and annual reports, and presentation data for the Office of Communication Security.

6. Reviews requisitions and issue slips prepared by operating divisions for availability of funds, and appropriateness of fiscal citations, and record notations.

OPERATIONS MANAGEMENT SECTION, AFSA-403C

1. Conducts a continuing management improvement program to assure conservation and utilization of manpower.

2. Devises and conducts work simplification and methods studies, evaluates the results of these studies and initiates the necessary action when and as required to insure that administration and production procedures are economical and efficient.

3. Analyze organization and proposed organizational changes for the Office of Communication Security.

4. Administers the allocation of space within the Office of Communication Security.

5. Devises and conducts a work measurement program suitable to the Office of Communication Security's production techniques and needs.

6. Administers within the Office of Communication Security the AFSA reports and forms control program.

7. Reviews operating division records of machine utilization for the purpose of taking action to improve utilization and develops machine replacement programs.

8. Recommends to Chief, Office of Communication Security, manpower allocations in accordance with long-range production plan based upon recommendations of the Planning Group and the operating divisions.

9. Administers efficiency awards program.

10. Conducts special management projects.

11. Originates and coordinates Personnel Relations Programs.

12. Coordinates specialized on-the-job training as required for AFSA-04 personnel.

ANALYSIS AND EVALUATION DIVISION, AFSA-41

~~—SECRET—~~

Establishes and promulgates the communication security doctrine of the Armed Forces; does this through the operation of two branches, with functions as follows:

TRANSMISSION SECURITY BRANCH, AFSA-411

1. Prepares policy, doctrine, techniques and instructional material applicable to the fields of transmission security, friendly traffic analysis and communications cover and deception which are within AFSA cognizance; reviews such material originated outside AFSA and forwarded to AFSA for coordination.
2. Reviews communications operating procedures to insure conformance with transmission security requirements.
3. Establishes policies designed to insure uniform Service enforcement of transmission security regulations.
4. Performs security monitoring of jointly utilized circuits; conducts analyses of traffic thus obtained; forwards results of such studies to the services as may be required.
5. Initiates requests to the Services for security monitoring of intra service circuits, maintains records concerning availability of Service security facilities to accomplish this.
6. Performs analysis of military communications for cover and deception programs.
7. Prepares new policies and executes established policies governing the use of strategic communications cover and deception: provides technical advice to cognizant Joint and Service agencies engaged in communications cover and deception.
8. Engages in planning of phases of strategic cover and deception programs; implementing those which are the responsibilities of AFSA. Provides as required special training and instruction to personnel engaged in communication deception activities.
9. Advises other AFSA organizations on matters pertaining to cryptologic countermeasures which are within the scope of AFSA responsibility.
10. Maintains surveillance of AFSA communications for the purpose of insuring maximum security. Devises procedures to insure security of AFSA communications.
11. Maintains liaison as appropriate with other AFSA organizations and other agencies.

EO 1.4. (c)
P.L. 86-36

66 ~~—SECRET—~~

~~SECRET~~

CRYPTOSEcurity BRANCH, AFSA-412

1. Recommends new cryptosecurity and physical security (of cryptomaterial) policies, and directs implementation in the Services of established policies in these fields.
2. Performs security and procedural evaluation of all existing and proposed cryptosystems and communications security mechanisms and devices.
3. Prescribes crypto-operating procedures, based on cryptanalytic studies, which will provide the maximum cryptosecurity compatible with operational requirements.
4. Establishes procedures for the reporting of violations of cryptosecurity and possible compromises of cryptomaterial by the Services; evaluates such reports and declares compromise when appropriate; initiates remedial action through Service channels, maintains appropriate records in connection with the foregoing.
5. Conducts programs of examination of encrypted traffic for violations of cryptosecurity. Makes arrangements through the Services for obtaining such traffic.
6. Prescribes the procedure for the submission of encrypted traffic reports; prepares studies based on such reports.
7. On request from non-military agencies, recommends special cryptosystems for their use and assists them in the formulation of their communication security policies and procedures.
8. Undertakes intelligence evaluation as necessary to insure proper evaluation of the security of U.S. cryptosystems in the light of foreign cryptanalytic potential.
9. Maintains liaison as appropriate with other AFSA organizations and other agencies.
10. Exercises technical control of cryptographic aspects of cover and deception.

CRYPTO-ENGINEERING DIVISION, AFSA-42

Performs basic engineering analysis with respect to planning production methods. Prepares engineering studies in methods and production control and efficiency of production methods. Performs fabrication, modification production testing, inspection, repair and maintenance of all crypto- mechanisms, keying elements, devices and equipment prior to issuance

~~SECRET~~

to using services and upon return therefrom. Prepares training manuals, course outlines, maintenance manuals, and replies to technical inquiries from the field.

Following is a breakdown by Sections of the functions of the Engineering Services Branch.

A. Equipment Standards Section (421B).

1. Prepares maintenance manuals, course outlines, training program, and training manuals for AFSA crypto- equipments.
2. Conducts training programs for maintenance personnel of the Branch and the Services.
3. Participates in service tests of crypto- equipment.
4. Analyzes equipment failure reports and initiates necessary corrective action.

B. Inspection Section (421C)

1. Inspects all crypto- equipments before issuance to the Services.
2. Inspects all rotors before issuances to the Services.

C. Fabrication Section (421D)

1. Rehabilitates, fabricates, and modifies all existing crypto- equipment issued by AFSA.
2. Rehabilitates all rotors received from the field.
3. Fabricates some of the new crypto- equipment issued by AFSA.

D. Rotor Section (421E)

1. Produces all rotors utilized by the Services.

E. Crypto Maintenance Section (421F)

1. Provides maintenance of Government owned teletypewriter and cryptoequipment for AFSA-13, AFSA-02, AFSA- 04, and Staff Divisions.
2. Provides maintenance on one time tape producing equipments.
3. Provides maintenance on rotor testing equipment.
4. Provides maintenance on AFSA-43 key producing and key checking equipments.

~~SECRET~~

F. Tape Section (421G)

1. Produces all one time tapes utilized by the Services.
2. Produces all M209 keys utilized by the Services.

Following is a breakdown by Sections of the functions of the Engineering Development Branch.

A. Machine Section (422B)

1. Manufactures parts for various types of communication equipments produced in AFSA and for supplying field agencies.
2. Manufactures parts for experimental models of communication devices and special production equipment for crypto accessories.
3. Provides maintenance services in AFSA-42 for shop equipment and special production equipment for crypto accessories.
4. Provides technical and manual assistance in the development of new production methods and new special equipment used in the production of crypto devices and components.
5. Designs and manufactures tools, jigs and fixtures for producing parts and for performing various operations in connection with the production of crypto accessories in the Engineering Services Branch.

B. Drafting Section (422C)

1. Prepares drawings of various types of permanent record for manufacture of parts for communications equipment produced in the Crypto-Engineering Division.
2. Prepares drawings for use as instruction manual illustrations and diagrams for equipments produced in AFSA or contracted for by AFSA. Detailed wiring diagrams of crypto equipments are also prepared.
3. Provides storage for and is responsible for security of all drawings produced in the Crypto-Engineering Division and those prepared for AFSA by private contractors.

~~SECRET~~

4. Sets up and maintains standards for modern and efficient drafting practices for AFSA and is responsible for disseminating such information to private contractors for their guidance in preparing drawings for AFSA.

5. Provides printing services for the Crypto Engineering Division and the Office of Communication Security in general.

C. Manufacturing Development Section (422D)

1. Designs and develops breadboard production models of new and modified classified communications equipment. Performs all engineering and trial test work necessary to arrive at a practical working model.

2. Designs, develops and builds special production and test devices for the Engineering Services Branch, AFSA-421.

3. Conducts life cycle tests on new equipments and components and recommends design changes based on these tests.

4. Provides general technical advice and engineering service for AFSA-04 and other AFSA units.

5. Maintains constant check on electrical power requirements and distribution, and provides technical help in connection with maintenance of electrical equipment.

D. Quality Control Section (422E)

1. Establishes and maintains a system of continuous quality control shop inspections for parts in process of manufacture.

2. Performs final inspection on all parts manufactured by AFSA and by outside contractors.

3. Performs and maintains a periodic and systematic inspection of all production tools and equipment.

4. Devises special methods, procedures and fixtures for inspection of unusually intricate parts or parts and assemblies held to very close tolerances.

~~SECRET~~

5. Endeavors to keep abreast with the latest methods in the field of Quality Control and in the use of special equipment.

6. Prepares and submits reports on final inspections performed.

Following is a breakdown by Sections of the functions of the Project and Material Requirements Branch.

A. Material Procurement and Stores Section (423B)

1. Initiates procurement for all items for which the Division is responsible.

2. Coordinates with project engineers material requirements for special projects and prepares supply forecasts.

3. Maintains complete and current project control records of property, equipment spare parts and associated items.

4. Prepares and distributes the cryptographic parts catalog used by AFSA and the Services.

5. Authorizes the release of parts and related items for AFSA projects, and other users of crypto-equipment.

6. Compiles material cost data for regular and special reports as required.

7. Maintains detailed procurement records, specifications and catalog reference file.

8. Provides custodial and miscellaneous supply services.

B. Project and Fiscal Accounting Section (423C)

1. Maintains personnel, time and attendance, labor and leave records. for AFSA-42.

2. Records and compiles cost data on assigned work projects.

3. Prepares and distributes monthly and special reports on work projects, production, fiscal and personnel status.

4. Records, verifies and distributes payroll checks and other personnel actions.

C. Office Services Section (423D)

~~SECRET~~

1. Performs a variety of clerical duties.
2. Prepares and maintains position control cards of assigned personnel.
3. Prepares and processes official personnel action correspondence.
4. Receives and distributes all incoming correspondence.
5. Sets up and maintains current correspondence and personnel records.
6. Prepares and distributes all official outgoing correspondence.
7. Maintains records and prepares requests for required forms.

D. Registered Publication Section (4231E)

1. Establishes and directs policies and procedures for the distribution and accounting of registered crypto- material.
2. Maintains detailed records as prescribed by the Department of Defense security regulations for the handling of registered crypto-material.
3. Receives, reviews and processes all requests for crypto-equipment and material.
4. Receives, stores and issues all registered crypto- material for the Division.
5. Prepares code cards for the wiring of rotors.
6. Assigns registry numbers for all crypto- equipments produced.
7. Responsible for the destruction of all registered and non-registered crypto-material.
8. Maintains a display of crypto-equipments.

CRYPTO-AIDS DIVISION, AFSA-43

1. Supervises and directs the activities of the various Branches within the Division which are responsible for the coordination of requests for programming, preparation, reproduction, storage, distribution and accounting of all crypto-material produced.
2. Exercises overall coordination control of the various branches in accomplishing the Division's assigned responsibilities.
3. Develops and coordinates the AFSA-43 portion of the overall AFSA-04 budget and mobilization plans.

~~SECRET~~

4. Receives, reviews, and processes requests for crypto material including rotors, tapes and pads for use by the U.S. Armed Forces, other U.S. Government Agencies, and certain allied governments.
5. Assigns nomenclature to Armed Forces Cryptographic systems, documents, machines, and related material.
6. Schedules the preparation and production including the determination of the reproductive process of cryptographic material.
7. Provides technical advice to other Divisions and offices as required.
8. Maintains stock levels and initiates procurement actions to obtain production equipment, material and supplies required for the production of printed cryptomaterial.
9. Maintains and supervises the Division cost accounting program.
10. Performs all civilian and military administrative functions within the Division.
11. Prepares recurring administrative and operational reports as required.
12. Maintains property accountability records for all property held within the Division.

PREPARATIONS BRANCH AFSA-432

Supervises and directs the activities of the various sections which are responsible for compilation, scheduling, machine processing, mock-up and cryptographic checking.

Following is a breakdown by Sections of the functions of the Preparations Branch.

a. Machine Processing Section (432B)

1. Operates IBM equipment with specialized devices in the preparation, processing and production of one time pads, codes, random scrambles, and other cryptographic documents.

b. Compilation and Scheduling Section (432C)

1. Initiates and schedules requests for production of cryptomaterial on a supersession basis.
2. Coordinates the format for all cryptographic documents and prepares letters of promulgation concerning their production, distribution and use.

~~SECRET~~

3. Develops and produces rotor wiring diagrams and cam contour patterns and provides cryptographic checks for all key lists using these items.

4. Maintains Master Control Records of all established cryptographic systems including the initiation, supersession rate, and compromises.

c. Mock-up Section (432D)

1. Translates original draft of cryptographic material into suitable form for lithographic processing.

2. Prepares materials needed for the reproduction of cryptographic material requiring limited distribution.

d. Checking Section (432E)

1. Engages in the cryptographic checking and proofreading of prepared materials prior to entering the reproduction process.

REPRODUCTION BRANCH, AFSA-443

Supervises and directs the sections responsible for photoplate making, offset and letterpress reproduction, and final finishing (binding) of printed material.

Following is a breakdown by Sections of the functions of the Reproduction Branch.

a. Photo Plate Section (433B)

1. Photographs for the purpose of producing lithographic plates all copy required to be reproduced by the offset printing method.

2. Reproduce by the photographic process special jobs for the various offices and Divisions within the Agency.

3. Prepares, strips and opaques negatives required for producing offset plates.

4. Sensitizes, exposes, and develops all lithographic plates used in the reproduction branch.

b. Offset Press Section (433C)

1. Reproduces by the offset method in quantity cryptographic and cryptologic material, forms, and miscellaneous printed items.

~~SECRET~~

c. Letter Press Section (433D)

1. Translates original draft of cryptographic and cryptologic material into suitable form for either letter press or lithographic processing.
2. Reproduces by the letter press method in quantity cryptographic and cryptologic material, forms and miscellaneous printed items.

d. Bindery Section (433E)

1. Provide all finishing operations for cryptomaterial produced by the offset press, letter press and machine processing section.
2. Visually checks all documents for completeness and quality.
3. Establishes accountability for all cryptographic documents by the assignment of register numbers.

DISTRIBUTION BRANCH, AFSA 434

Supervises and directs the operation of the various sections concerned with the storage, distribution and accounting of registered cryptographic materials.

Following is a breakdown by Sections of the functions of the Distribution Branch.

a. Routing and Records Section (434B)

1. Maintains master accounting records covering the bulk distribution of registered cryptographic documents of the Armed Forces, other U.S. Governmental Agencies and Allied Governments.
2. Accounts for all registered cryptographic documents to custodians within the Agency.
3. Maintains historical library of all registered crypto documents.

b. Storage and Shipping Sections (434C)

1. Inventories all cryptographic material received for distribution.
2. Provides limited storage of registered cryptomaterial as required.
3. Makes necessary arrangements for receipt and dispatch of cryptomaterial.
4. Issues registered cryptographic material to custodians within the Agency.

~~SECRET~~

Equipment

Part II, A.4

Prior to the start of World War II, manual systems, which had carried the main load of communications security, were gradually replaced by wired rotor machines. During the next several years rotor machines became the standard cipher devices for high level traffic. At lower echelons, for example, below Army division level, manual systems continued to be used, with the M209¹, a mechanical device, carrying the bulk of encrypted communications. As tape productions became more efficient and more economical, one time tapes came to be used more heavily, but it is likely that they carried no more than 10% of all encryption.

The securing of voice communications continued to present major difficulties for the technicians of the day. By the beginning of 1943, the SIGSALY, a ponderous on-line voice encryption system, had been installed at about a dozen sites around the world, including Washington and London. It was used on a few occasions for talks between Roosevelt and Churchill, but the system worked poorly and suffered from problems such as low-grade voice quality, synchronization difficulties, and power level fluctuations. The SIGSALY used vacuum tubes, but used rotors as part of the keying process. Although it represented a major step forward in voice encryption technology, it actually was used only sparingly and was scrapped with the war's end.

A few other speech systems based on vacuum tube technology were developed during World War II, but none of these played a significant role. Some, notably the Navy ASAX-2 and the Army AN/IFSC-2/3 (a trailer mounted voice system) employed sets of revolving discs for generation of key.

Rotor machines held swag until advancing technology in the form of transistors, magnetic binaues, and miniaturized components started the downward trend, but certainly not the demise, of rotors. Rotors and new technology shared a sort of phase-out, phase-in process over a period of about twenty years. Communications bit rates had increased far beyond those which could be accommodated by rotors for on-line encryption, and the need for voice encryption had grown

~~SECRET~~

significantly. Electronic cryptography was developed and employed to cover these areas first. For off-line purposes, the SIGABA/ECM₁, and the modified version, TSEC/KI-29, continued in use through the 1950s². The Combined Cipher Machine (CCM), was used by the United States, England, and other allied nations. The U.S. stopped use of the CCM in 1960, but it was continued in use by NATO until about 1966. The TSEC KI-7/47 had about a 20-year life span, to the mid 1970s, for the U.S., and about a 30-year life span for NATO.

Machines using wired rotors remained as the foundation of U.S. cryptography into the 1950s, and rotors served to complement other technologies well into the 1970s.

ROTORS AND ROTOR DEVELOPMENTS

In the decade following World War II, the United States engaged in an extensive program for the development of rotors, principally for electro-mechanical cryptographic equipment. However, this development program had been materially reduced by 1960. Although the rotor had been one of the most versatile and powerful cryptographic tools available in the field of machine cryptography, the serious limitations of electro-mechanical rotor machines (principally speed limitations, inflexibility once basic design parameters had been established, and the extended production and tooling time required) caused them to be generally supplanted by electronic equipments. In addition, the extremely expensive operation of wiring rotors and issuing new sets to the field mitigated against their continued widespread use.

Equipments, devices, and the rotors for use in them continued to be considered however, on a limited scale for tactical use where small size and ruggedness were of prime importance. Development also continued to a limited extent on higher echelon rotor equipments until the electronic developments in this field completely proved themselves as far as practical operation and ease of maintenance were concerned.

Following is a brief summary of the background of specific rotor developments on COMSEC equipment in the U.S.¹

As has been noted, the invention of the rotor as a basic component in the encrypting/decrypting operation in mechanical and electro-mechanical cipher equipments

~~SECRET~~

represented a major milestone in the history of machine cryptography. Available evidence seems to indicate that the wired rotor was originally conceived by H. A. Koch, a Dutch inventor, during the years immediately preceeding World War I, and it found its first practical embodiment in the German "Enigma" machine. Almost simultaneously, and probably independently, it was invented and patented in a somewhat different form by E. H. Heburn, an American. One additional feature of Heburn's effort was that, in wiring his rotors he obtained

Another concurrent, and again perhaps independent, contribution to the art was made by Sidney Hole, a farmer from Devonshire, England, who developed and patented a cipher machine which utilized pneumatic rotors.

EO 1.4.(c)
P.L. 86-36

The subsequent history of the development of electrical wired rotors in the U.S. is one of evolutionary progress through the succeeding years. In the latter 1920's the U.S. Navy contracted with Heburn to build a wired rotor cipher machine for military use. The first results of this development were not completely successful and, because of legal difficulties of a patent and contractual nature, no further work was performed by Heburn for the U.S. Government. In the years immediately preceeding World War II, however, an equipment was evolved which was to become the major high echelon cipher equipment used by the U.S. in World War II. It was based upon the concept of a wired rotor maze and included the principle of enciphered motion¹ developed by Mr. W. F. Friedman and Mr. Frank Rowlett. Under the direction of Captain L. F. Safford, U.S.N., Teletype Corporation developed and produced this equipment, known in the Navy as the CSP-889 or Electric Cipher Machine (ECM), and in the Army as the SIGABA, or converter M-134-C. In contrast to the evolutionary development of the wired electrical rotor, the pneumatic rotor approach of Hole was not advanced until the basic principle of a pneumatic rotor was applied to the development of the TSEC/KI-17, a small, literal cipher machine.

The two types of wired rotors, as used in the German "Enigma" and in Heburn's machine, had certain basically different characteristics, and subsequent rotor developments were identified as Hebern-type rotors or Enigma-type rotors according to these characteristics. The Hebern type

~~SECRET~~

rotor had flush electrical contacts on each of its surfaces and it fit between fixed separates which contained spring loaded contacts. These contacts pressed against the flush contacts of the rotor to make circuit continuity through the maze. The Enigma-type rotor had flush contacts on only one face, and spring loaded contacts on the other face which pressed directly against the flush contacts of the adjacent rotor to make circuit continuity through the maze. Thus, no fixed separators were required in equipments employing the Enigma-type rotor. The Hebern type rotor became the basic component of the high level literal and teletypewriter security device used by the U.S. in World War II and the Korean war (with the exception of one time type devices). The Enigma type rotor had been used in most of the British and German cipher machines, and was the primary component of the literal equipments developed in the U.S. and other major countries in later years.

The rotor thus became one of the most useful and versatile cryptographic tools during the span from 1941 to 1955. Cryptographically, it afforded a very high security potential, particularly when used as an interchangeable component in a "permuted maze" system; physically, it was a compact, rugged, and relatively simple device. For all of their good attributes, however, there were limitations in the services which rotors could provide. Among these limitations were 1) because rotors had to be stepped mechanically, their operating speed was relatively slow, and as a result their application was confined to devices with a maximum speed requirement of between 60 words per minute; 2) contact resistance build-up and dimensional instability of rotor bodies were major problems; 3) cryptographic security standards, and advances in cryptanalytic techniques - including the application of high speed analytic machine processes to rotor machine solution - proved that a maze of ten rotors was the minimum number which could be permitted in an acceptable crypto-system; 4)

Further, the cost of initial manufacture, or wiring and rewiring, and of distribution was high in both time and money.

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

HEBERN TYPE WIRED ROTOR DEVELOPMENTS BLUE ROTOR

This 26-point rotor was the basic rotor used in U.S. cipher machines during World War II and up to the late 1950s. The Blue Rotor was a typical Hebern rotor. It was used in the SIGABA/CSP-889 series of equipments, of which about 11,000 were made; the CSP 1700 series of equipments, of which about 2,000 were made; and the ASAM 2-1 series of equipments, of which about 2,500 were made. It had the important advantages of being simple and rugged with very few parts, but it was relatively large (3-1/2" diameter x 5/8") and heavy (6 oz.). The fact that the Blue Rotor required separators in the maze, thus doubling the number of electrical contacts per circuit path through the maze, required greatly increased power to cope with the increased circuit resistances thereby created. The manual rewiring required of this rotor was a relatively slow process, and at critical times in the history of its use the rotor wiring out barely kept up with requirements. In the "Colmar Incident"¹ of World War II, the wiring of the Blue Rotors and replacement rotors in use in the European Theatre of Operations were considered compromised. This necessitated the special assignment of the equivalent of a battalion of men working on a crash basis to rewire Blue Rotors to permit continued use of the cipher equipment in that area. Another disadvantage of the Blue Rotor was the fact that other than rewiring it, the only

WHITE ROTOR

On order to give the Blue Rotor a greater number of

a modification was introduced in March 1952. Existing

Blue Rotors were modified to accept an alphabet ring and a notch ring for controlling rotor stepping, both of which could be rotated with respect to the main rotor body and which could be freely interchanged from one rotor body to another. This modified Blue Rotor was called the White Rotor.

YELLOW ROTOR

As part of the development of the TSEC/KI-47 by the Navy, a small, 26-point Hebern type rotor, designated the Yellow Rotor, was built. However, for reasons of economy and logistics, NSA

EO 1.4.(c)
P.L. 86-36

80-~~SECRET~~

~~SECRET~~

decided to modify the KL-47 to accept the existing Red Rotors¹ thus negating the need to go into production on the Yellow Rotor.

ENIGMA-TYPE WIRED ROTOR DEVELOPMENTS GREEN ROTOR

Near the close of World War II a 26 point Enigma-type rotor was developed for use in a small, battery powered cipher device known as the SIGFOY (M-325). This equipment was never used operationally, but an improved version of its rotor, known as the Green Rotor, was employed in an on-line, teletypewriter equipment called the SIGNIN. A rotor of the Enigma-type, with the consequent elimination of separators, made possible a much smaller maze than in earlier U.S. electro-mechanical cipher equipments, and the rotor was designed to be rewirable without soldering to speed up the wiring process. This was achieved by making it possible to shift some of the internal mechanisms by hand into any one of 26 positions. Four hundred and fifty SIGNIN's were produced by the end of World War II, and some were still in operational use as late as 1958.

RED ROTOR

The development of the Red Rotor represented the major U.S. effort in this field in the post World War II era. A Series of cryptologic studies initiated in February 1946 resulted in the decision to use a 36-point rotor with rotatable notch rings and alphabet rings as the basic cryptographic component of two new cipher machine developments, an off-line literal security equipment, TSEC/KL-7, and an on-line teletypewriter equipment, TSEC/KW-9. The 36-point rotor was chosen in order that a common rotor could be used in both systems.

Technicians working on these systems encountered two major problems during development of the Red Rotor. One was contact resistance build-up, and the other was dimensional instability of the plastics being used. The Red Rotor used beryllium copper and, in operation, particles wore off which turned into copper oxide. Copper oxide is very abrasive; this caused the wear effect to be cumulative. It is also non-conductive, and the build up on contact points caused interference with proper operation of the cipher maze. Problems with the plastics used in the Red Rotors came about because of the wide tolerances of parts. These conditions were attributed to the

~~SECRET~~

methods used in the molding process, as well as the environmental situations in which the equipments were used.

Starting in 1946, four contractors were assigned to studying Red Rotor developmental problems. During the following ten years more than a million and a quarter dollars were spent on research relating to the Red Rotor and its successor, thus Orange Rotor. A thorough evaluation of nearly 200 contact materials did not uncover a better material for practiced application than the original material, beryllium copper; and a lengthy search of plastic compounds showed that the one used in the original Red Rotor design was the most suitable for the purpose. Follow-on equipment modifications and improvements enabled the Red Rotor to be fully acceptable in all of the machines designed to use it, namely, the TSEC/KL-7, TSEC/KL-47, and TSEC-KW-9.

ORANGE ROTOR

Orange Rotor was a Red Rotor with some changes. The principal change was that a metal hub was added to positively space the rotors, the alphabet ring was made rotatable without having to remove it from the rotor, and the notch ring was made wider and sturdier. The Orange Rotor went into production in August in 1956 and at that time was designated as the standard 36-point wired rotor.

BROWN ROTOR

Development of the Brown Rotor, undertaken by the Navy with NSA approval, was completed by the end of 1954. The differences between the Brown and the Red Rotors were principally in detail design. Because it was so basically similar to the Red Rotor, for which production tooling had been completed, the Brown Rotor was not considered for production.

PRINTED ROTOR DEVELOPMENTS

In 1946, as a parallel approach to the development of the Red Rotor, technicians initiated a study on the feasibility of using a printed rotor to meet existing requirements. In the laboratory models that were built, the printed circuitry was etched on the rotor body itself. The aim was to have printed circuit rotors for the TSEC/KL-7 and TSEC/KW-9 be the same in physical appearance and outside dimensions as the wired rotors. In this way, complete interchangeability of printed

~~SECRET~~

circuit and wired rotors in the machines using the Red Rotor would be possible. In view of this, the basic printed rotor approach was dropped and a development was pursued in which mixed wiring inside a Red Rotor was replaced by a plastic disc containing printed mixed circuitry. Outward appearance of the rotor with the printed circuit insert was the same as that of the rotor with mixed wiring. At the time that the decision was made to go into production on the TSEC/KL-7 and the TSEC/KW-9 because of the emergency brought on by the Korean War, a decision also had to be made on whether to go into production on the wired Red Rotor or on the printed circuit insert. The users decided that since they had invested considerably more time in testing and developing the wired rotor, they would proceed with that choice. Development continued on the printed circuit disc, but at a low priority, and was concluded in 1953. NSA used the pilot equipment for experimental and educational purposes for awhile, but ultimately discontinued the project.

PNEUMATIC ROTOR DEVELOPMENT

In 1949, a pneumatic rotor was developed for use in the TSEC/KL-17, a small, keyboard operated literal cipher machine requiring no source of external power other than manual. This rotor was basically an Enigma-type rotor in which the mixed electrical wiring was replaced by air passageways. Pneumatic circuits, instead of electrical circuits, were established through the rotors comprising the maze.

By 1958 there were no plans for further contractual research and development activities on wired rotors. On the basis of past results technicians concluded that no significant improvement in the wired, 36-point rotor could be expected, either in the basic design approach of the Orange Rotor, or in more radical changes to that design. Local research continued at NSA on a low priority basis whenever an approach seemed to hold sufficient promise of marked improvement over the existing designs.

One effort which was continued for awhile involved a search for a conductive plastic. This was researched by the Markite Corporation and showed promise of resulting in a plastic to replace the metal contacts being molded into the plastic rotors. It was felt that the problems encountered by the differences in expansion between metal and plastic in the rotors could be alleviated by the

~~SECRET~~

use of conductive plastic parts, and possibly a much smaller rotor could be achieved. This project, designated CALLIOPE, was eventually dropped.

Work on printed rotors for use in the TSEC/KI-98 and the TSEC/KI-3 continued. This effort resulted in a rotor for use in low echelon, low speed, manual devices. The use of this rotor in power driven equipment was evaluated through its application in the TSEC/KI-7 modification aimed at achieving interoperability with the TSEC/KI-17.

Termination of the studies on conductive plastics and printed rotors signalled the definite de-emphasis of rotors as a major cryptographic tool of general applicability in communications security equipment.

Rotor Development, Post World War II

<u>Rotor</u>	<u>Manufacturer</u>	<u>Covered Fiscal Years</u>
Red/Orange Rotor	Molded Insulation Co.; Minneapolis Honeywell Regulator Co.; American Phenolic Corp.	1947 through 1956
White Rotor	American Molded Products; Lundquist Tool and Manufacturing Co.	1952-1953
Printed Rotor	Melpar Inc; General Mills, Inc.	1954 through 1957
Flammable Plastic (for a plastic suitable for rotor use which would make it possible to readily destroy rotors in an emergency by incendiary means)	Esselen Research Division of U.S. Testing Corp.	1952-1953
Pneumatic Rotor (for KI-17)	Corning Glass Works; Mycalex Corp.; Pure Carbon Co.	1954-1957
Blue Rotor	National Scientific Labs; Sterling Eng. Co.	1954-1956
CALLIOPE (development of a conductive plastic for rotors)	Markite Co.	1956-1957

HIGH AND MEDIUM GRADE CIPHER MACHINES IN USE

84-~~SECRET~~

~~SECRET~~

Converter M-134-A, short title SIGMY, and its successor, Converter M-134-C, short title SIGABA (U.S. Navy designation: Electric Cipher Machine, or CSP887) were the mainstays of U.S. communications security prior to and during World War II. The United States Army's and Navy's "Security line" in cryptography was ably and successfully defended and maintained by the SIGABA, one of the best, if not the best, high grade cipher machines of its time. England and America owe a great debt to their cryptanalysts for their efforts in winning the cryptanalytic phase of World War II, but a great debt is also due those persons whose skill and ability in cryptography resulted in providing the United States with SIGABA. The United States began to win the cryptographic war with the invention and development of converter M-134-A, SIGMYC, between 1935 and 1938. It was regarded at that time as a good machine, perhaps providing adequate security. Continued study, modification, and design, in which work both the Army and Navy contributed, resulted in the development of Converter M-134-C, SIGABA. The SIGABA embodied a cryptographic principle (5-rotor device) never before used in any cipher machine. Yet the development was not achieved easily, for the project encountered almost insurmountable difficulties. The chief difficulty was obtaining adequate funding to defray the necessary costs of improving the machine. It was fortunate that SIGABA was ready for use at the time when it was most needed because subsequent experience demonstrated that SIGMYC would not have proved practical enough for the extensive demands imposed upon communications facilities with the outbreak of World War II. The SIGMY consisted of two units connected together, a typewriter and a cryptodevice. The only function of the typewriter was to furnish a printed copy of the plain or cipher text. Encipherment was performed by the cryptodevice, utilizing five rotors which were stepped by a long key tape. Later, because the use of key tapes proved impractical, stepping of the rotors was accomplished by means of a keying unit, short title SIGGOO.

Only a few of the SIGMYC converters were produced. Before the war the SIGMYC was used by the Army on only a few circuits, mainly between Washington, Fort Shafter (Honolulu), Quarry Heights (Panama), and London. Although the SIGMYC afforded about the same degree of

85 ~~SECRET~~

~~SECRET~~

security to communications on which it was used as did the SIGABA, mechanical and operational features of the machine made it impractical for wartime military usage.

The Converter M-134-C, SIGABA, using a five rotor mechanism for enciphering/deciphering, was similar in cryptographic principle to the ISGMYC. It differed, however, in the manner and means by which stepping of the cipher rotors was carried out.

The SIGABA was used exclusively by the Army and the Navy. Starting with only a few equipments in 1942, the Army had more than 3,200 machines by the end of the war. The Navy had considerably more than this number.

As a result of investigation and interrogation of many German cryptographies and cryptanalysts, it was concluded that the German's had no success in their attacks on SIGABA traffic, nor did they have information regarding the appearance or operating principle of SIGABA. They referred to it as the "American Machine," or as "AM-2," but the most that they could discern from examination and study of intercepted traffic was that the U.S. had a highly secure, high-grade cipher machine. This fact is borne out by the interrogation by Specialist Dr. Ferdinand Vaegele, Chief of Section E of the Signal Intelligence Agency of the Commander in Chief of the Air Force and principal cryptanalyst in the German Air Force, who stated that he "...did not know the name of this machine and had no idea of its appearance or operating principle. As with Typex, no success was achieved and attempts to break the system were dropped."¹

Lieutenant Martin Ludwig, an evaluator of the Signal Intelligence Agency of the Air Force High Command, when questioned concerning cryptanalytic attacks upon SIGABA, stated:

"Vigorous efforts were made to break it, especially by the German Army. Army experts considered decipherment possible right up to the end of the war."²

As far as can be determined, in the absence of work sheets or formal reports, the cryptanalytic attack on SIGABA was in the nature of [REDACTED]

[REDACTED] in an attempt to discover the basic cryptographic characteristics of the machine.

Although this fact is not stated definitely in any of the interrogations, such as attack is along the

EO 1.4.(c)
P.L. 86-36

86 ~~SECRET~~

~~SECRET~~

same line of procedure as that followed in the case of the Combined Cipher Machine (CCM) and TYPEX.

SECURITY OF ROTOR MACHINES

Three factors formed a defense line against exploitation of U.S. rotor machines:¹

1. The opponent had to know precisely how the cryptographic machine process worked;
2. he had to acquire, or to reconstruct, wiring for the applicable rotors, and,
3. he needed the key list information.

Even though strong measures were used to keep each machine safe from compromise, from the time that a machine was put into use it was accepted that sooner or later that machine, or its essentials, would become known to opponent countries. It was further accepted that such an event could occur without the U.S. being aware of it; and even if it were known, there could be no sudden replacement of the machine. Therefore, it was determined from the beginning that each rotor machine type would be so designed as to be safe for use even after a foreign power came into physical possession of one of them. All decisions on actions needed to counter the effects of a physical compromise of rotors or of key lists, or of a cryptographic "list", took into account the possibility that a major opponent already knew precisely how the cryptographic machine process worked.

Each rotor set had a shorter life - one to three years of actual use - and a narrower distribution than the machine itself. Every rotor set and every rotor was protected by strong physical and personnel security measures. yet when some event occurred which was judged to permit successful reading of traffic if rotors were known to the opponent, the action taken might be based on the possibility that the rotors were known. For example, if a copy of a key list was reported missing and unaccounted for and the corresponding rotor set was a widely held one that had been in use for one or two years, the messages encrypted in that key list might be declared to be compromised. In that case all holders were requested to review the affected messages for any action which might ease the damage from compromise. Similarly, if a cryptographic "bust occurred

~~SECRET~~

that would enable reading of messages by a foreign party who happened to have the rotor set and know the machine details, messages in the key involved probably would be declared to be compromised.

The key list was considered the most critical of the three lines of defense. Any suspicion surrounding a copy of the key list, from its inception to its destruction, was reason for prompt and serious actions. With few exceptions, compromise of a key list was viewed as tantamount to compromise of all traffic encrypted in that key list. Reserve keys were kept in position for prompt supercession. For a majority of such incidents the supercession was usually billed as precautionary, with no message review requested; but declaration of compromise along with a request for message review was not a rare occurrence.

Despite the basic assumption that sooner or later a major opponent would manage to get a SIGABA/ECM, a CCM, or any one of the other rotor machines, and despite actual incidents of possible compromise, the time never arrived at which the U.S. gave up the protective measures aimed at keeping rotor machines safe from physical compromise.

Primary cryptographic systems which continued to be used for a number of years following their successful employment during World War II were in addition to the Army Converter M-134-SIGABA and the Army high security teletypewriter cipher system SIGTOT; the Army speech equipment RX-220-T1 SIGSALY; the Combined Cipher machine, CCM; the Navy electrical cipher machine Mark III, ECM - same as SIGABA; the Navy teletypewriter cryptographic attachment, CSP1515 - same as Army Converter 228, and the Army teletypewriter cipher attachment known as Converter M228 SIGCUM. Converter M-228 was a machine, developed by the Army, which made possible simultaneous and instantaneous encipherment, transmission, reception, decipherment, and printing of teletype communications either by wire or radio. For radio transmissions, the machine was allowed to be used only in RESTRICTED and CONFIDENTIAL communications, although on wire lines in U.S. controlled, friendly territory: SECRET material could be passed via this means.

88 ~~SECRET~~

~~SECRET~~

The SIGCUM machine enabled the Army to pass a very large amount of intercept traffic by radio, accurately and expeditiously, from various intercept centers to the Signal Security Agency.

The SIGABA was a rather heavy equipment, used a lot of electric current and was not well suited to use in the field. During World War II, the Army expressed a requirement for a field type equipment which would be light enough to be easily transported, rugged enough to take field activity treatment and yet provide the degree of security demanded of operations. This requirement was met by a machine invented by a Swedish engineer named Boris Hagelin. One hundred thousand of these machines, designated the M-209, were produced by the Smith Corona Typewriter Corporation during the period 1942 - 1944. It had some mechanical deficiencies and a few cryptographic weaknesses, but it was nevertheless, the best field equipment extant, and was used extensively by the Armed Forces during the war and for some time thereafter.

The SIGABA and the M-209 were off-line equipments. Output of both was a gummed tape containing either enciphered or plain text depending on the operation being performed. The gummed tape was then posted onto a message form. This type of off line operation had two major weaknesses: first, it was too slow; second, it increased the possibility of operator errors. These off-line equipments required operator handling of both plain text and enciphered text at each end of the communications circuit. In the first step the plain text was typed into the crypto-equipment, which produced an enciphered text on gummed tape. The enciphered text was posted onto a message form and then transmitted as a separate and additional operation - either the operator of the crypto-equipment or the transmitting operator could, and did, make errors. At the receive end, the operator received the enciphered message which, in a next step operation, had to be deciphered by the crypto-equipment. This off-line operation was too cumbersome for increasingly modernized communications, and had the added serious disadvantage of increasing the number of operator errors because of the additional handling step involved.

Around about the mid 1950s, it became accepted fact that growing requirements for rapid secure communications could only be met with on-line systems. These systems provided for

~~SECRET~~

simultaneous encipherment and transmission at one end of the circuit, and simultaneous receipt and decipherment at the other end. From the operator's viewpoint, then, the task was simply to type plain text into the transmitting end of the circuit and plain text would come out at the receiving end. He was not concerned mechanically with the encipherment and decipherment processes which took place in between.

The earliest beginnings of on line operation can be traced back to the World War I era. At that time an AT and T engineer named Gilbert Vernam came up with the idea of a punched tape teletypewriter security system. Several equipments using this punched tape system were fabricated and tested just before the war's end with the termination of hostilities, interest lagged and there were no funds for further development. The equipment used at first a single loop of punched tape, and then two loops of punched tape in changing combinations to produce random cryptographic key for encipherment. Both the single loop and two loop techniques proved to be cryptographically insecure, and the alternative of going to a one time tape system was considered impractical because of the problems involved in distributing the tape. In any event, at the beginning of World War II not one of these equipments was in existence. But with the beginning of World War II, plans for the equipment were resurrected and the machines were produced as a priority task. As they were further developed during the war the equipments used either one time punched tape or rotors to provide cryptokey to mix with the plain text.

During the mid-1950s NSA produced the KW-26, an electronic equipment which represented a major departure from the previous electromechanical punched tape and rotor equipments. The KW-26 is a fixed plant, on-line teletypewriter security equipment which has been used extensively. It was built during the vacuum tubes-to-transistors transitional period. Bi-magnetic cores were the principle circuit components, but miniature vacuum tubes and transistors were also used. Some of the major important improvements introduced by the KW-26 were: 1) being an on-line device, it reduced operator errors and was inherently faster, being used at speeds of up to 100 words per minute, 2) it used a built in electronic key generator and eliminated the employment of the more cumbersome rotors and one-time tapes 3) it used pluggable printed circuit

90-~~SECRET~~

~~SECRET~~

boards and packages which could rapidly be replaced to restore an equipment to operational use. It was no longer necessary to locate and replace the individual defective part before an equipment could be made operational after being removed from service. It was simply a matter of isolating the board causing trouble and replacing it with a board known to be good. Identification of the defective component and replacement of it on the board could be done in the workshop, and at a convenient time. Placing an equipment back into operational condition was thus reduced to a matter of minutes, instead of hours or days.

Introduction of the KW-26 into the arsenal of cryptoequipments designed to maintain the integrity of U.S. communications was the act which opened the door on the -----technological advance in communications and cryptographic systems which continues to this day.

SIGABA

The SIGABA, or Electric Cipher Machine (ECM), the most effective U.S. cipher machine of its time, was used on those nets which demanded the highest protection of information. This machine was held as U.S. Eyes Only from the time it was introduced until the early 1950s, at which time it was released to the U.K. and Canada.

Approximately 11,000 SIGABA's were built during World War II. The machine contained two 26-point mazes, one of which performed the encipher/decipher function, while the other controlled the stepping of the alphabet maze. Not only was the SIGABA an extremely secure and dependable device, it was also highly versatile. Through the use of various rotor arrangements, switches, and other special adaptors, it could be made to encrypt/decrypt numerical weather data, to be used as the Combined Cipher Machine (CCM), and to be used as the short-lived Backward Combined Cipher Machine (BCM).

By the late 1940s, Army and Navy COMSEC elements decided that the machine needed to be modified and strengthened. This judgement was based on the fact that significant advances had been made in the field of cryptanalysis during the decade, both in the areas of human knowledge and technological application. The resultant revised version of the SIGABA was called BACchus. During its long and useful lifetime this most important machine was identified by a

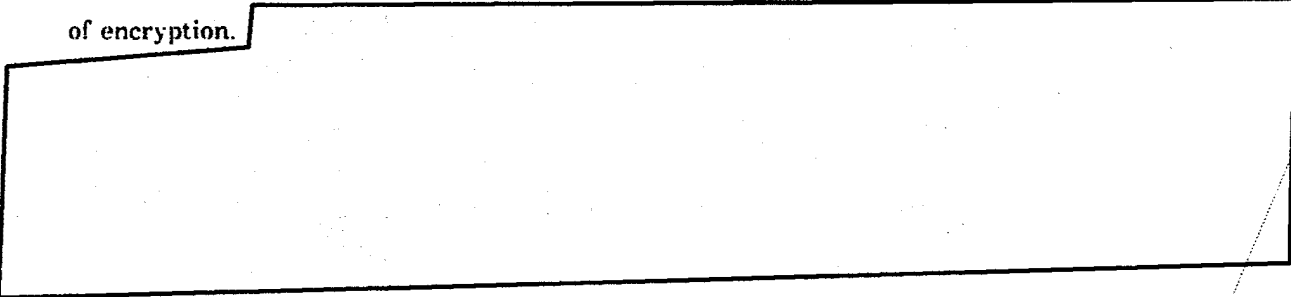
~~SECRET~~

number of short titles, including Converter M-134C; CSP 888/889; CSP 2900; ASAM-1; and those above, i.e., SIGABA, Electric Cipher Machine, CCM, BCM, and BACCHUS.

COMBINED CIPHER MACHINE (CCM)

The CCM was designed early in World War II to encrypt allied communications. The British CCM off-line mainstay was a machine designated Type X (TYPEX), a five rotor machine with mechanical activation of rotor stepping. A CCM maze was designed for a basket imposed on the TYPEX and for another basket that was fitted into the SIGABA. This modified version of the SIGABA was known as AJAX. By 1954 approximately 2000 CCMs had been made from chassis of the CSP 889 models of SIGABA, 200 more were made from new parts.

Extensive cryptanalysis on the system from 1943 onward coupled with close following of usage and of operator error in use of the system, led to periodic revisions in the procedural processes of encryption.



The CCM was withdrawn from use starting about 1955. Replacement was made on a continuing basis as sufficient quantities of the next generation of cipher machines came along. The new machines, designated TSEC KI-7/KI-47, to replace the CCM in NATO in late 1958.

EO 1.4.(c)
P.L. 86-36

TSEC KI-7/KI-47

By the end of World War II, the Army Security Agency had readied requirements for the development of a new, portable, off-line, rotor machine. Early requirements for such an equipment were aimed at Army division and Air Force equivalent elements, with the intent of providing more convenient, faster, and more secure encipherment than was then available for such levels. Small size, simplicity of procedures, and portability were the attributes emphasized. The ASA efforts resulted in a design that included a new 36-point rotor and a new machine, the TSEC KI-7.

~~SECRET~~

While the KI-7 was still in development, plans were made for two levels of usage. One, called POLLUX, was for tactical applications. This was defined as field Army equivalent and below, and operational procedures called for clear text message indicators and fixed set of six rotors. The other level of usage was termed ADONIS. The ADONIS system provided for enciphered message indicators and a box of ten rotors, from which the six needed could be drawn.

While ASA was developing the KI-7, the Navy COMSEC organization under the design direction of Captain Lawrence F. Stafford was seeking a new rotor machine for shipboard use. With the centralization of COMSEC development, and the formation of AFSA, General Canine, Director of AFSA, decided that the new Army and Navy machines would be cryptographically compatible, to the point of providing inter-communication. In early 1952, the Army originated logic was chosen as the basis for both machines. This was the genesis of the Navy's TSEC KI-47. While the Navy continued with the development of a machine which would fit specifically the shipboard environment, AFSA continued development of the Army originated machine, with emphasis on providing an equipment that would be suitable to field environments. Keying materials for the Navys KI-47 were as prescribed for the Army's KI-7, as were enciphering/deciphering procedures.

KW-9/AFSAM-9

This on-line system was developed in parallel with the off-line KI-7, and used the same 36-point type rotor. Keying materials were essentially the same as for the KI-7; one method of use (ATHENA) employed clear text message indicators, and another method of use (IRIS) employed encrypted message indicators.

The KW-9 was used only sparingly, for less than ten years. It was secure enough, but it had maintenance problems which significantly affected its reliability.

COMBINED CIPHER MACHINE (CCM)

The Combined Cipher Machine (CCM), introduced in 1944, was designed specifically to fill the need for a common cryptographic system for use between the U.S. Army/Navy and the British military. For both security and operational reasons, it was necessary to have a high grade

~~SECRET~~

cipher system by which a large volume of traffic could be handled but which would not endanger or compromise Converter M-134-C, SIGABA. It was not possible to permit the British forces to have access to the U.S. SIGABA, nor to an inappropriately modified machine from which they might have been able to reconstruct the cryptographic principle of SIGABA. The Combined Cipher Machine, derived from the SIGABA chassis but employing a totally different cryptographic principle fulfilled the requirement for a Secure cryptographic machine while at the same time safeguarding U.S. cryptographic secrets.

TSEC-KL-17

The hope of developing a rotor cryptomachine which would operate without electrical power of any kind, accept keyboard input, provide printed output, and be safe against cryptanalysis, persisted for many years. Such a device was needed for low echelon tactical operations where electricity was either not available or not dependable. In 1948, an AFSA engineer named Albert Small, came up with the idea of a pneumatically operated cipher machine. This was designated the TSEC KL-17, also known as the DEM-17. The device was a small, keyboard-operated, tape printing rotor machine in which the functions of the electrical signal current were effectively reproduced by a pneumatic system. Each rotor contained a system of air passages, or air tubes. When the rotors were properly installed and aligned, twenty-six pneumatic passages through the maze were created. Air pressure was generated by tiny bellows, one of which was located under each key of the keyboard. Finger pressure on the key was sufficient to operate a print after the air found its path through the maze. Output was printed on 3/8 inch paper tape. The approximate weight of the TSEC KL-17 was nine pounds, and the overall dimensions were 8" x 8" x 4".

About 12 of the devices were produced for test purposes. It worked well mechanically, but users found it sluggish in its operations. Also, the degree of finger pressure needed was a bit more than that required for a typewriter, and this proved to be troublesome. The KL-17 probably would have been competitive had it been produced earlier, say during World War II, but by the mid-1950s, when it would finally have been ready to go, consumers were looking for greater

~~SECRET~~

convenience than it could provide. The machine was never put into production and the project was eventually abandoned.

BCM (Backwards CCM)

The BCM, a modification of the Combined Cipher Machine, was designed by Captain Lawrence F. Stafford about 1950. The BCM had six rotors, two of which stepped in reverse direction. The BCM was competing with the TSEC/K1-7, which had been under development for several years. At the beginning of 1952 General Canine reviewed the two equipments and decided that the Navy's BCM should be cryptographically compatible with the K1-7, but that it could be a separate development aimed at shipboard equipment. This judgement resulted in the action leading to development of the TSEC/K1-17 and the BCM concept was dropped.

MCB

The MCB was a 5-rotor machine designed and used by the Department of State. It was cryptographically similar to the CCM in its procedures for encryption. Primary applications of the MCB were for embassies and attaches, locations at which the U.S. was unwilling to risk the SIGABA/ECM. The machine went out of use in the late 1950s and was replaced by the MEC-1 and one-time tape systems.

MEC-1

In the early 1950s the Deputy Secretary of State, Lee W. Parks, designed a rotor machine based on the SIGABA/ECM. His objective was to adopt as much of the SIGABA logic as was needed to achieve sound security, but at the same time avoid risking the SIGABA details in the hazardous locations in which the Department of State had to use its cryptographic machines. He presented the logic to AFSA COMSEC experts for engineering design. The machine went into use in the late 1950s and was used until 1964, when it was replaced by more modern electronic systems.

MX-747, SIGBRAT

At the end of World War II Civil Defense was a large part of U.S. defense planning. The organizational elements of Civil Defense had need for cryptography but could not provide the level of physical protection required for cryptomachines or the personnel clearances normally required.

~~SECRET~~

The SIGBRAT was built from SIGABAs to fill this purpose, but there was considerable controversy over whether or not it was sufficiently secure for the job intended. This indecision resulted in only a few being constructed, and those were in use for only a short time.

CSP 1511

During World War II plastic, inflammable, water-proof cellulose acetate trips were manufactured and issued as the CSP 1511 series for use by amphibious forces. However, these strips were not generally accepted nor used for their intended purpose, probably because any strip system is unsatisfactory when it is to be used under the adverse conditions encountered in most amphibious operations. This strip, whose only advantage over paper lay in the fact that it was relatively impervious to water, had several disadvantages, chief among them being that the difficulty and expense - plus production delays - would be out of all proportion to the benefits to be derived.

~~SECRET~~

References for Equipment

A lightweight, ruggedized Swedish designed machine manufactured by Smith Corona Typewriter Company. M-209 was the Army's designator for this equipment; CSP-500, the Navy's.

The SIGABA, known as Converter M-134-C (U.S. Navy designation: Electric Cipher Machine (ECM), or CSP 889 was the most successful and secure crypto machine used during World War II.

See SRH-359, A History of Converter M-134-C.

A History of the Wired Rotor in U.S. Communications Security, by Ryon Page, will be updated and published by the History and Publications Branch.

Machine Cryptographic and Modern Cryptanalysis, Cipher Deavour, Louis Krugh. pp. 6.
Artech House, Dedham, Mass. 12850

Get info on

Summary attached

The Colmar incident occurred during World War II when a French farmer from Colmar, France, stole a military vehicle with an operational SIGABA on board. The farmer dumped the SIGABA and its accompanying rotor sets into a nearby river. As a result of this action, SIGABA rotors in use and programmed for use in the European Theatre were declared compromised. When the cipher machine and rotors were recovered from the river, close examination seemed to indicate that the thief had not penetrated the protective cases of the SIGABA and rotors, but the compromise declaration stood and the massive task of wiring and distributing a whole new batch of rotors was carried out.

History of the SSA, Volume VIII, Chapter V.

Ibid.

Ibid.

The wired rotors in U.S. COMSEC, Ryon Page, VI. F. 21