

NSA review(s) completed.

BEST COPY

Available

THROUGHOUT

FOLDER

5/47/62
Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
TOP SECRET

THIS DOCUMENT CONTAINS CODE WORD MATERIAL

COMMISSION ON ORGANIZATION OF THE
EXECUTIVE BRANCH OF THE GOVERNMENT

TASK FORCE REPORT
ON
INTELLIGENCE ACTIVITIES

APPENDIX I

MAY 1955

THIS DOCUMENT CONTAINS CODE WORD MATERIAL

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
TOP SECRET

SEC. CLASS.	SPINTE			CONTROL NO.	Appendix # I
DATE OF DOC	DATE REC'D	DATE OUT	SUSPENSE DATE	CROSS REFERENCE OR POINT OF FILING	
May 1955				ER report # 14.E.	
TO	Appendix I, Part I, Report of Survey of National Security Agency and Appendix I, Part 2, Report of Survey of Communications and Electronics (Clark Task Force Report) (Staff Documents File)				ROUTING
FROM					
SUBJ.					
COURIER NO.	ANSWERED	NO REPLY	2		

6			
ACTION	DIRECT REPLY	PREPARE REPLY	
APPROVAL	DISPATCH	RECOMMENDATION	
COMMENT	FILE	RETURN	
CONCURRENCE	INFORMATION	SIGNATURE	

Remarks:

We are once again returning Appendix I of the Clark Task Force Report on Intelligence Activities as it requires special handling. For your information, we are retiring the other parts of this report in the Records Center.

FILE COPY - RETURN TO EXECUTIVE REGISTRY.

ER acquired this from SPINTE files now under complete See complete job 70-B-626 Bot # 24

These records are to be held intact and when no longer needed are to be returned to the Agency Archives and Records Center under job: 70-S-626

SPECIAL INTELLIGENCE STAFF, DD/S&T

FOLD HERE TO RETURN TO SENDER

FROM: NAME, ADDRESS AND PHONE NO.	DATE
LBKirkpatrick/ []	14 Apr 62
UNCLASSIFIED	CONFIDENTIAL
	SECRET

RETURN TO SPINT 25X1
CIA

TOP SECRET

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

THIS DOCUMENT CONTAINS INFORMATION RELATED TO COMMUNICATIONS INTELLIGENCE AND MUST BE HANDLED AND STORED SEPARATELY FROM OTHER TOP SECRET MATERIAL, WITH ACCESS LIMITED TO THOSE PERSONS DESIGNATED BY NAME ONLY.

THIS DOCUMENT CONTAINS CODE WORD MATERIAL

TOP SECRET

TOP SECRET

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

APPENDIX I, PART 1

REPORT OF SURVEY OF NATIONAL SECURITY AGENCY

BY

RICHARD P. OVENSINE, BRIG. GEN., U.S. ARMY, RETIRED

AND

ROBERT J. FOLEY

APPENDIX I, PART 2

REPORT OF SURVEY OF COMMUNICATIONS AND ELECTRONICS

BY

TERENCE J. TULLY, BRIG. GEN., U.S. ARMY, RETIRED

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

TOP SECRET

TOP SECRET

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

Clarke Task Force
Report on

INTELLIGENCE ACTIVITIES

in the

FEDERAL GOVERNMENT

Prepared for the

COMMISSION ON ORGANIZATION OF THE
EXECUTIVE BRANCH OF THE GOVERNMENT

by the

TASK FORCE ON INTELLIGENCE ACTIVITIES

APPENDIX I

Part 1

THE NATIONAL SECURITY AGENCY

MAY 1955

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

TOP SECRET

APPENDIX I

Part 1

THE NATIONAL SECURITY AGENCY

TABLE OF CONTENTS

	<u>Page</u>
I GENERAL	1
II ORGANIZATION AND OPERATIONS	8
III SECURITY	19
IV RESEARCH AND PLANNING	24
V PERSONNEL AND TRAINING	27
VI LOGISTICS	39
VII ELECTRONICS INTELLIGENCE	41
VIII RECOMMENDATIONS	46
IX GLOSSARY OF TERMS AND ABBREVIATIONS	58

TOP SECRET

TOP SECRET

I GENERAL

Scope of Survey

This survey covers communications intelligence, communications security, electronics intelligence, and their relationship to the intelligence community. The substance of this report is classified as a special category of TOP SECRET and the contents must not be revealed to anyone who has not been specifically cleared and indoctrinated to receive communications intelligence. These papers should be handled and stored separately from other TOP SECRET material.

In accomplishing the survey, the task force endeavored to assess the value and necessity of the communications intelligence effort now being exerted by the United States and identify and analyze major problems whose solution requires external actions to be taken in order to obtain maximum results with minimum expenditures of time, personnel, and money.

In the course of this survey, a staff team visited the National Security Agency, the Army Security Agency, the Naval Security Group, the Office of Special Operations of the Department of Defense, the Office of Assistant Chief of Staff, G-2, of the Army, the Office of Naval Intelligence, and the Office of Air Force Intelligence in Washington, D.C.; the Vint Hill Farm Station in Virginia; the Air Force Security Service at Kelley Air Force Base at San Antonio, Texas; and the Air Force Technical Intelligence Center at Wright-Patterson Air Force Base at Dayton, Ohio. One member of the team made a trip to Europe with members of the task force. Numerous briefings were given the team and a far greater number of individuals were individually interviewed. The team spent most of its time with NSA, visiting all

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

TOP SECRET

echelons from the Director to the working levels. In all, more than 200 individuals talked to the team in varying degrees and were interviewed by the team.

Definition of Communications Intelligence

Before proceeding further, we should define the subject of this discussion. "Communications intelligence," commonly known as COMINT, as used herein, is defined to mean all procedures and methods used in the interception of telecommunications, the obtaining of information from such communications by other than the intended recipients, and the product thus obtained.

Historical Development of COMINT

The COMINT effort of the United States today is a vast undertaking whose estimated cost approximates an annual expenditure of about

This modern giant has grown through natural evolution from quite modest beginnings. It is an offspring of our electrical and electronic age. Rudiments of the art were developed in the Civil War with the secret tapping, by both sides, of telegraph lines. The use of radio communications, however, in World War I probably marked the beginning of modern COMINT.

Following World War I, the Army and Navy, in separate operations, began to intercept radio communications of foreign nations and to study and develop the related field of cryptology. These operations were continued on a very modest scale until the outbreak of World War II when the Army and Navy each rapidly expanded its efforts. The wartime effort was outstandingly successful and constituted a most valuable element of military intelligence. The wartime experiences pointed out, however, the need for coordination between the two services

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
regarding channels each should have for exchange
of technical information of value in the decryption of intercepted
messages.

Such voluntary cooperation as was developed during the war was obviously inadequate. After the cessation of hostilities, the Army and Navy combined forces to form the Armed Forces Security Agency (AFSA). This was a rather loose federation in which the director did not have operational control. Despite his lack of authority, considerable progress was made in bringing about some coordination of effort between the two services. As the experiences of AFSA indicated greater benefits to be derived from a truly unified operation which AFSA was unable to develop with its limited authority, and in view of the development of an Air Force COMINT activity which was completely dissociated from AFSA, a survey of the situation was made by a special committee appointed by the President, known as the Brownell Committee. The recommendations of that committee were followed with only minor variations and the present organization of the National Security Agency, together with the policy board structure to guide it, has now been in operation for more than two years.

The COMINT effort has grown under NSA. The number of intercept positions has increased in two years from [redacted] Today about 25X3
[redacted] messages are intercepted each month. The daily receipts of this traffic arriving by air courier in Washington amount to about one ton of paper in addition to approximately [redacted] groups of 25X3
encrypted radio traffic.

Estimates of intelligence agencies as to the portion of finished intelligence which is derived from COMINT vary from 10 percent to 95 percent. Although these estimates indicate that an important element

TOP SECRET

of some fields of intelligence is dependent upon COMINT, the most significant fact appears to be that the intelligence community, without exception, was emphatic that the COMINT product should not be diminished, but, on the contrary, should be increased, if practicable.

The present COMINT effort, mammoth as it is, does not accomplish or even approach a complete interception of all foreign radio traffic. The program now in effect calls for an increase from manned intercept positions by the end of fiscal year 1957. This increase still will not permit complete coverage, but it should close some important gaps in the present coverage. The widespread dependence of the modern world upon telecommunications, the continuing state of cold war, the rigid controls of the police states of the Communist orbit, and the lack of other dependable information which would disclose the capabilities and intentions of our adversaries combine to create the necessity for a large-scale COMINT operation. Today, about individuals are engaged in the collection, analysis, and distribution of COMINT. This organization supplements other sources of intelligence, including covert and overt activities. It constitutes a form of insurance for the United States whereby it is hoped and expected that some advance warning will be obtained concerning hostile acts and intentions, on a large scale, of the Soviet orbit.

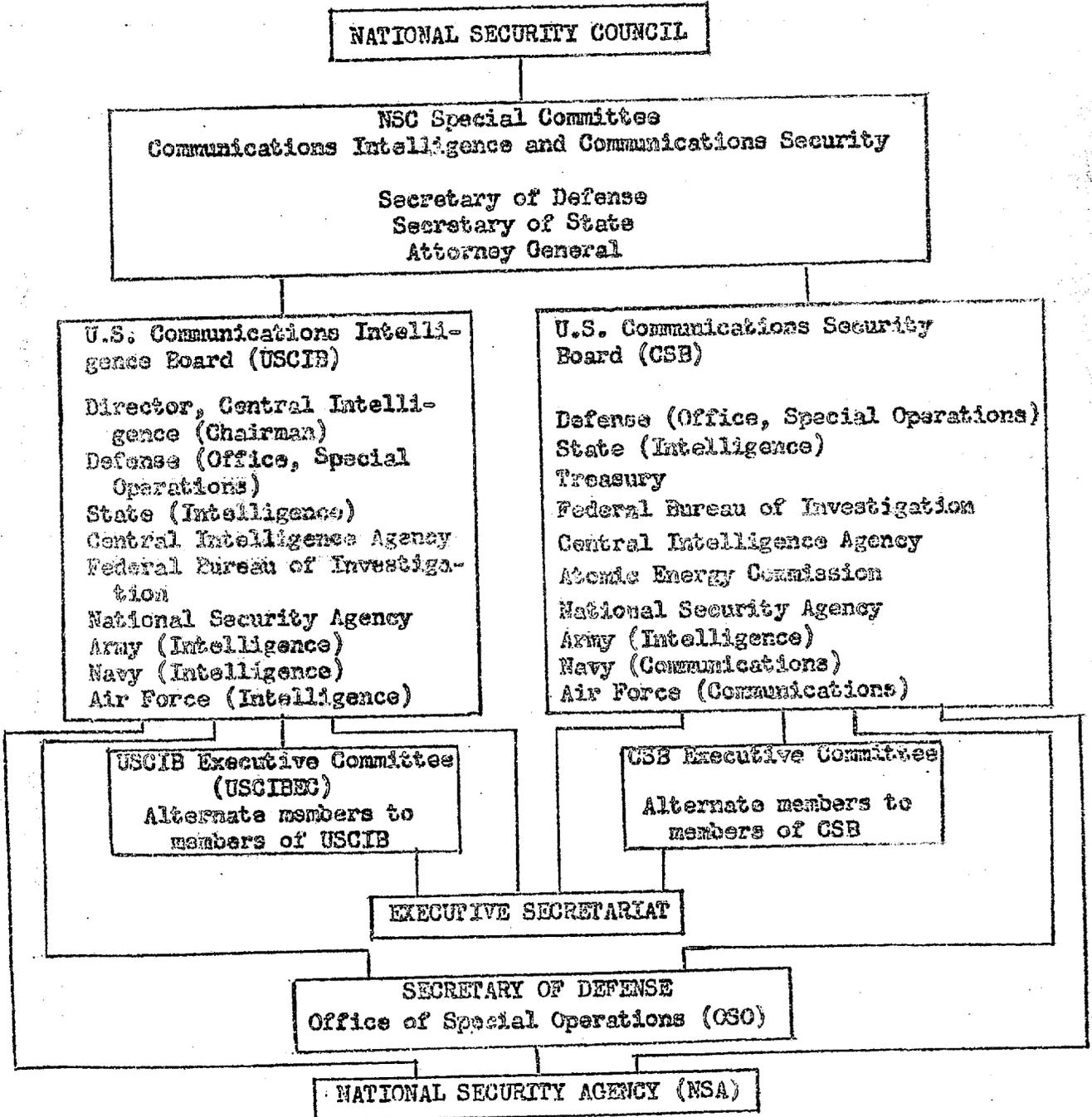
25X3

25X3

TOP SECRET

Policy Structure

COMMUNICATIONS INTELLIGENCE AND SECURITY POLICY STRUCTURE



Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
TOP SECRET
The organization governing the communications intelligence and communications security operations is graphically portrayed above.

The basic directives setting up this structure are contained in National Security Council Intelligence Directive Number 9 (NSCID No. 9), dated December 29, 1952, for communications intelligence and National Security Council Directive Number 168 (NSC 168), dated October 20, 1953, for communications security. These directives resulted from the Brownell Committee.

In this structure, it was intended that the Special Committee for NSC act upon basic policy matters and resolve disagreements which arise within the two policy boards under it; it acts as the ultimate arbiter in communications intelligence and security matters. The Communications Intelligence Board (USCIB) receives for its guidance the statements of National Intelligence Objectives and Requirements formulated by the Director of Central Intelligence after concurrence by the Intelligence Advisory Committee. USCIB thereupon publishes a Master Requirements List, with supplements, which is intended to be the basis for NSA intercept operations.

The Secretary of Defense is designated as the executive agent under the two policy boards. He has, in turn, delegated his authority relating to direction and control of the operations of NSA to the Assistant to the Secretary of Defense (Special Operations), and the Office of Special Operations constitutes the link between the Department of Defense and the National Security Agency. NSA is the agency which executes or implements the directives and missions which are handed down to it. Through the Office of Special Operations, the Director, NSA, can, when appropriate, express his views directly to the top echelon within the Department of Defense.

TOP SECRET

The statements of National Intelligence Objectives and Requirements are framed by the Director of Central Intelligence, with concurrence of the Intelligence Advisory Committee, in broad, general terms, but these do not specifically state which agency shall do what particular task in the collection of information. Each department and agency, therefore, makes its own decision as to what effort it shall devote toward each of the intelligence objectives and requirements.

USCIB has endeavored to cover all objectives and requirements with COMINT, but has been unable to cover the requirements in statements of specific tasks to be accomplished by NSA. In practice, NSA receives a statement of objectives and priorities from USCIB which compares in bulk with the Washington telephone directory. The basic guidance which NSA thus receives from USCIB is a Master Requirements List which requires NSA to provide exhaustive information on every conceivable subject. It takes no cognizance of the capabilities and limitations of NSA and requests information far beyond the capability of that agency. It is amplified by eight Information Requirements Lists.

USCIB is aware of the difficulties imposed on NSA by the scope of the Master Requirements Lists and Information Requirements Lists which have been furnished that agency and USCIB has, in recent months, attempted to formulate more adequate guidance for NSA. It is too early to determine whether the new directives will be adequate.

Because of the failure of USCIB to provide a clear operations order for the Director, NSA, it has devolved upon representatives of the intelligence community and NSA to develop at the working level a plan for the interception and analysis of COMINT. This has proved to be unsatisfactory.

TOP SECRET

Communications intelligence and communications security are recognized as related facets of telecommunications, yet policy guidance is determined by two boards - the U. S. Communications Intelligence Board for intelligence and the U. S. Communications Security Board for security. Agency membership on both boards is essentially the same, except that AEC and Treasury are members of the USCSE but do not participate on USCIB. A single secretariat services both boards and NSA is the implementing agency for both communications intelligence and communications security.

II ORGANIZATION AND OPERATIONS

Organization of the National Security Agency

NSA is the agency which executes or implements, in accordance with directives from the policy making boards, the assigned communications intelligence and security tasks and missions, under the direction of the Secretary of Defense (OSO). The agency is headed by a Director, currently a lieutenant general, U. S. Army. It is composed, in addition to its headquarters, staff, and support personnel, of three major elements: communications intelligence, communications security, and research and development, each under a Deputy Director.

The agency at this time is located in three places - one part is co-located with the Naval Security Group on Nebraska Avenue, Washington, D.C., and a second part is located with the Army Security Agency at Arlington Hall Station, Arlington, Virginia. The NSA is badly overcrowded in this situation and is consequently forced to operate a shift from about 4 p.m. to midnight. This unsatisfactory condition will be remedied when the NSA is moved to Fort Meade, Maryland, where barracks and operating space are under construction. The smallest,

TOP SECRET

January 1955. The move to Fort Meade should be completed about December 1956.

The National Security Agency is primarily a producer of information as distinguished from evaluated, integrated intelligence. Its position, therefore, is that of a service agency to, and not a member of, the intelligence community. The Director derives his missions from the intelligence community as represented in USCIB (the Director of NSA is also a member of that board). The broad mission of NSA in the COMINT field is to intercept transmissions emanating from foreign sources, to process that intercept (including decryption and translation), and to disseminate the processed COMINT to authorized elements of the intelligence community.

It is a fact, however, that NSA does produce for the intelligence community more than unevaluated raw material. Due to the tremendous volume of intercept material, NSA must winnow out a great deal of it as worthless - this is a process of evaluation. Because of the nature of much of the intercept, NSA also compiles studies which represent the accumulated knowledge gained from a mass of individually insignificant messages. This, too, involves evaluation of the material and the deduction of conclusions; it is done by NSA rather than by members of the intelligence community simply as a matter of expediency. Regardless of the fact that NSA conducts some intelligence processing, the recipients of its product are responsible for its evaluation in the light of such other information as may be available to them.

The Director of NSA is not a member of the Intelligence Advisory Committee. He is strongly of the opinion, however, that he should be at least a non-voting member in order that he might understand the motives and reasons back of the directives he receives from USCIB, to assist in

his exercise of judgment in the day-to-day decisions which must be made in implementing the broad directives and priorities received from USCIB.

COMINT Operations

The COMINT missions of NSA consume its major effort, both as to the number of persons engaged and as to the funds involved. Virtually all NSA personnel are located in the Washington, D.C. area; subordinate headquarters, relatively small, are located in the United Kingdom, Europe, Alaska, the Far East, and the Pacific (Hawaii). The actual interception of telecommunications is accomplished in the field, almost entirely overseas (including Alaska), by elements of the Army Security Agency (ASA), the Naval Security Group (NSG), and the Air Force Security Service (AFSS).

These cryptologic services in October 1952 maintained [] manned positions, which number had been increased in November 1954 to [] and is planned to reach [] in June 1957. These positions are presently grouped in [] intercept stations which vary in size from a single position to as many as [] positions of various types capable of copying manual or automatic Morse transmissions, [] radio printer, radio teletype, and voice. About [] separate messages are intercepted every month in addition to about an equal amount of operators' chatter and other transmissions which are not strictly messages. The vast bulk of this traffic, amounting to [] of paper per day, is sent to Washington by air courier. Traffic of a more urgent nature is sent to Washington by radio. The NSA communications center has [] direct on-line circuits, with [] stations or headquarters having other direct on-line circuits, which thus connect NSA with a total of []

25X3
25X3
25X3
25X3
25X3
25X3
25X3
25X3
25X3
25X3

25X3
25X3

TOP SECRET

stations or headquarters. In October 1952, the NSA communications center handled a daily average of about 932,000 groups, and in October 1954, of about 1,271,000 groups. NSA receives or sends about 70 percent of all encrypted traffic flowing in and out of Washington. It is expected that the personnel strength of the four cryptologic organizations on June 30, 1955 will be:

25X3

25X3

The Director, NSA, is authorized operational and technical control and such administrative control as he deems necessary over the cryptologic units of the three services. He has delegated operational control and responsibility for processing the intercept in some instances to a major cryptologic organization of each of the three armed services in Europe and in the Far East. He also has delegated responsibility for the long-range Soviet air force to the Commanding General, U. S. Air Force Security Service, together with operational control over specified Air Force cryptologic units designated for that purpose. With that one exception, neither operational orders to the elements in the field nor the messages which they intercept are passed through the headquarters of Army Security Agency, Naval Security Group, or Air Force Security Service, which makes those headquarters administrative, not operational. It is the plan of the Director, NSA, to effect further decentralization as rapidly as the elements in the field are sufficiently trained and equipped. Approximately twelve processing problems have been given to various stations and groups located outside continental United States. The purpose of decentralization is to process intercept material as far forward as practicable in order to expedite delivery to field commanders of the information with which they are concerned, and to reduce

25X1

the volume of electrical communications to and from Washington. Decentralization of processing has the effect of delaying the receipt in NSA of the traffic which is processed overseas and it results in some duplication of effort. However, the advantages of decentralization of processing to stations which are capable of performing that function appear to outweigh the disadvantages in that the economies of centralized processing are less important than the reduction in time of delivery of information to the field commanders concerned. Furthermore, the reduced burden on communications to and from Washington would provide economies of considerable importance.

The matter of operational control over intercept units appears to be the only serious point of disagreement between members of the intelligence community - specifically the Navy and the Air Force - on the one hand and NSA on the other. The chiefs of intelligence of the Navy and the Air Force have expressed a desire that NSA issue only mission-type orders to the chiefs of the three cryptologic services and that operational control of the intercept units (with certain positions reserved to NSA control) remain with those services. It was, however, such a relationship in the Armed Forces Security Agency (AFSA) that demonstrated the need for the reorganization resulting in the creation of NSA. The change in operational control proposed by officers of the Navy and the Air Force ignores the confluence of service interest in intercept frequencies as illustrated by the following:

25X1

TOP SECRET

primary interest in COMINT; (3) operations are not economical or effective when some Soviet links have to be copied two or three times and others not at all; and (4) NSA alone has the necessary machines and the technically qualified personnel to process some of the more sophisticated intercept. The present organization is designed to give field commanders the information which is of concern to them directly from the intercept unit which receives or first reads the intercept at the same time that the information is passed to NSA. The point from which such information is disseminated, through Special Security Officer channels, is the point at which the intercept is processed, and, under the NSA plan of decentralization, is the farthest forward practicable, which is determined by the availability of qualified personnel plus the degree of sophistication of the intercepted system.

The Director, NSA, exercises operational control over the selection of locations for new intercept stations, but has not conducted inspections either before or after installation of the intercept stations and there seems to be a question as to whether he has authority for such inspections. Some fixed stations have been laid out in the past, especially in the period before establishment of NSA, in such manner that maximum efficiency in interception is not attainable. Loss of efficiency has been brought about in some instances through establishment of a station intended to serve both for normal service traffic and for interception of COMINT traffic. In other instances, the intercept missions have been changed to directions for which the original layout was not intended. NSA and the cryptologic services are aware of these and other technical problems, but difficulties have been encountered, and not yet completely solved, in the construction of some fixed stations.

Position of the Cryptologic Services in the Armed Forces

The positions of the three cryptologic services in the Armed Forces are all different. The AFSS is a separate command of the Air Force, directly under the Chief of Staff, on the same level with the other major commands; the ASA is an agency of the Army under the Assistant Chief of Staff, G-2; and the NSG is under the Chief of Naval Intelligence for operational control and the Director of Naval Communications for all other matters, including personnel and logistics. The importance of the organizational structure extends far beyond the position on a chart. It is of primary importance in the assignment of personnel, which is so often a compromise between conflicting interests. The cloak of secrecy which necessarily surrounds the cryptologic services has kept the personnel offices of the Armed Forces in ignorance of the true importance of such assignments.

The matter of logistical support also suffers when a minor command or agency has to compete against a major command in the face of an overall shortage.

Special Security Officers

In order to provide a link whereby COMINT may be passed to commanders who have need for such information and have been specifically indoctrinated and cleared therefor, there has been established in each of the Armed Forces a system of Special Security Officers (SSO). An SSO detachment, consisting of one or more officers together with enlisted assistants, is located so as to form the communications channel between a cryptologic processing unit and the headquarters which that unit supports. The SSO is actually a member of the cryptologic service, not of the supported command, but he is authorized to work with the headquarters of the supported

TOP SECRET

unit and may, if so desired by the supported commander, serve as an additional member of the latter's intelligence division. The SSO is responsible for advising the supported commander regarding all security aspects of the COMINT delivered to the commander.

The Recipients of COMINT

There is established within the office of each of the intelligence community recipients of COMINT (State, Army, Navy, Air Force, and CIA) a special COMINT section, established within a secure area and all of whose personnel are cleared and indoctrinated for COMINT. It is the function of these sections to receive, evaluate, and recommend action to be taken on the communications intelligence which they receive from NSA. They correlate COMINT with other information and prepare intelligence reports.

Each of the intelligence agencies mentioned above also maintains a liaison detachment with NSA, physically located adjacent to the production element, but with some restrictions upon their access to individuals at the working levels. The COMINT sections mentioned above receive COMINT through these liaison detachments and also through direct teletype lines and messenger service from NSA to the COMINT intelligence sections. In practice, the liaison detachments know what is sent to their respective intelligence offices, but the actual transmission may pass direct from the NSA production elements to the intelligence offices.

The size, mission, and operations of these five liaison detachments vary considerably. From small detachments established for the purpose of improving mutual understanding between the producers and recipients of COMINT through the obtaining of answers to specific questions, indicating points where further information is desired, and assisting the intelligence

agencies in their utilization of COMINT, all but the State Department detachment have gradually grown and assumed additional functions to where the Air Force detachment, especially, is now preparing intelligence reports in final form, and other detachments are doing original work.

Three priorities committees have been set up within NSA, composed of members of NSA production elements and members of the liaison detachments. It was intended that these committees serve as groups wherein the NSA technicians would be kept fully advised of the reasons underlying information requirements, so as to assist in the arrival at logical decisions regarding NSA operations, and the liaison detachments would be kept advised as to the technical implementation by NSA of the USCIB requirements. In practice, this has not been satisfactory to either party. Because of the failure of USCIB to provide adequate guidance to NSA in the form of tasks and priorities, these committees have attempted to fill the void. NSA, however, has not received the information it desires from the liaison detachments, possibly because the latter are too far removed from their chief of intelligence and are unable to represent his point of view. These committees have been unable to agree on what products to eliminate or curtail in order to obtain more of another product and the liaison detachments have been unable to make decisions based on an overall appreciation of the intelligence requirements - their viewpoint has been too restricted. In this situation the liaison detachments have attempted to exert a direct influence on the operations of NSA through contacts at the working level.

A considerable degree of friction has developed between the liaison detachments, or some members of those detachments, on the one hand, and members of NSA at the working levels, on the other hand.

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
 The presently authorized strengths of these liaison detachments

are:

Army	
Navy	
Air Force	
CIA	
State	
Total	

25X3

The present for duty strengths are slightly less.

Reports

The reports rendered by NSA fall into two groups - intelligence reports which are intended for the intelligence community and technical reports which are designed to aid the intercept and analytic personnel of the cryptologic services.

The intelligence reports include spot reports submitted by intercept units or NSA whenever information received or read is considered of sufficient importance to warrant immediate attention of the field commander or the intelligence community; O/GEN's, which are weekly reports containing a fusion of information developed during the period; and special reports, which cover a wide field and are based upon studies, sometimes over a period of several months, which develop information from a large mass of intercept, the individual pieces of which are of no significance. Special reports are developed in accordance with the requirements of the intelligence community and may, if desired, be kept up to date on a recurring report basis.

Technical reports cover matters such as radio net diagrams, call signs, identification of code systems, information about transmitters, etc.

The NSA Technical Support Catalog of December 1, 1954, which includes both intelligence and technical reports, lists 428 reports, of which the

TOP SECRET

great majority are recurring.

The COMINT Product

All members of the intelligence community have expressed an ardent desire for a constant flow of timely translations of messages of the Communist orbit which will be indicative of future plans and intentions. Our successes in reading Japanese and German high-level traffic during World War II and our success in reading a large portion of Russian Communist [redacted] until 1948 have led the recipients of COMINT to expect a continuation of such successes. [redacted]



The effectiveness of COMINT is primarily dependent on top-level mathematicians, cryptanalysts, systems analysts, and other types of professional people. There are extremely few individuals today who combine a high degree of knowledge and skill in all of these fields. An increased effort in one problem area, therefore, usually demands some diminution of effort in another, and the Director, NSA, has experienced difficulty in properly allocating his top-flight personnel because of the exhaustive requirements levied on NSA by the intelligence agencies.

18
TOP SECRET

25X3

25X3

25X3

TOP SECRET

III SECURITY

Communications Security

The basic directive for communications security (COMSEC) is NSC 168. NSA performs its COMSEC missions through the procurement, manufacture, or printing, and issue of certain cryptographic equipment, devices, and publications, or approval of equipment or systems; through the publication of policies, doctrines, and instructions governing the use of cryptographic material; and through supervision of the manner in which cryptographic material and systems are used by the various departments and agencies of the Government. Most of the cryptographic devices produced by NSA are actually manufactured by private industry under contracts with NSA. The agency itself manufactures certain top secret parts of those machines in a production plant operated within its own area by its own personnel; those critical parts are later inserted in the machines built under contract. NSA also operates its own printing and reproduction plant for the production of one-time pads and other highly sensitive cryptographic material.

NSA, furthermore, has fulfilled certain commitments of the United States to the North Atlantic Treaty Organization concerning communications security.

The material and systems used by the departments and agencies of the Federal Government are believed to afford adequate communications security and are of such nature that errors in their use probably do not permit the decrypting or reading by unauthorized persons of more than the one message or part thereof involved in each error or violation of security. However, numerous tests made by communications security personnel have disclosed that great quantities of highly valuable information not avail-

able from other sources are available to foreign governments through traffic analysis and messages sent in plain text. In this latter respect, the United States should be presumed to have a very low degree of communications security.

The Director, NSA, has recognized this weakness and has initiated action toward the development of equipment to make all telecommunications secure. This is a long-range research and development project, however, and probably will not be completed in less than five years. Our present communications facilities cannot cope with a much greater load than they now carry in encrypted traffic.

In addition to the probable release of valuable information through traffic analysis and plain text messages mentioned above, actual breaches of security involving encrypted systems have occurred and presumably are still occurring. During the twelve months from March 1, 1954 to February 28, 1955, 1,331 cases of possible compromise of telecommunications were reported to NSA. These cases included 850 possible cryptographic compromises, 261 possible physical compromises of cryptographic information, and 220 possible compromises of COMINT due to transmission insecurity. Of these possible compromises, NSA concluded that there were 234 probable compromises. An evaluation of these probable compromises indicated that there were 26 cryptographic compromises which probably resulted in the compromise of 23 single messages, the compromise of one day's traffic in each of two systems, and the compromise of one system normally used for one month. Possible compromises, other than cryptographic, were 64 physical compromises (exposure of codes, keys, or publications) and 144 cases of transmission insecurity (of which about eighty percent were operators' errors).

TOP SECRET

When compared with the total number of encrypted messages transmitted, the number of possible compromises is an extremely small percentage. The possible intelligence value to an unfriendly power derived from the loss of communications security in even a few cases is not susceptible of accurate evaluation; it could be of great value.

The Director, NSA, does not actually monitor United States transmissions - the monitoring is conducted separately by each service or agency. Neither does he have authority to set standards on transmission security. It does not appear to the task force that he should have authority to establish communications procedures, which necessarily vary among the services and agencies. Consideration should be given, however, to the possible granting of authority to the Director, NSA, to prescribe minimum standards for development of communications procedures which will provide and maintain security of transmissions. Such authority, if granted, could be subject to review by the Communications Security Board.

All violations which could have resulted in a compromise of communications security are reported to the Director, NSA. Disciplinary actions in connection with security violations are the responsibility of the Director, NSA, only when they concern NSA personnel. Such actions are taken by the chiefs of the three cryptologic services concerning their own personnel without reference to NSA.

Examining the matter of communications security, which is intimately connected with intelligence and particularly communications intelligence, it soon became apparent that communications security cannot be viewed alone, but must be considered as part of the entire telecommunications field. In this vast field there are many committees, boards, and agencies,

TOP SECRET

each concerned with some facet or segment of communications, but they are not tied together in a coordinated effort. The Telecommunications Planning Committee, under the Office of Defense Mobilization, is the nearest approach, apparently, but it does not fill the void which now exists.

NSC 168 does not clearly define the responsibility and authority of the Director, NSA, and insure that the entire subject of communications security is adequately covered.

Internal Security

Closely related to communications security is the matter of internal security of NSA. The physical areas in which COMINT is produced or held, normally, are restricted areas to which persons are admitted only when properly authorized. Communications concerning COMINT are transmitted either by courier or by electrical transmissions using special cryptographic devices or codes restricted solely to COMINT.

Personnel on duty with or allowed access to COMINT are given complete security clearance and indoctrination prior to commencing such duty and their security records, including a National Agency check, are subsequently reviewed at five-year intervals. Complete field investigations have not been repeated at five-year intervals. During the periods between reviews of records, NSA conducts an educational program to remind its personnel of the security aspects of their work and to urge all individuals to report all violations or suspicious circumstances.

The number of American individuals now cleared for COMINT follows:

TOP SECRET

25X3

Recipients of COMINT
Producers of COMINT (cryptologic
services)
Special weather service per-
sonnel
Civilian consultants throughout
the United States

Total



These numbers are so large as to constitute a constant danger to the security of COMINT operations. The steady turnover of personnel in the COMINT activities results in the continuous flow of large numbers back to civilian life throughout the United States. Surveillance is not maintained over these civilians after they have left NSA service. Because of the obvious threat to the security of COMINT created by the large number of persons cleared for such information, various measures have been devised to minimize this danger.

In the first place, all individuals cleared for COMINT are not granted access to all COMINT matters; the "need-to-know" rule is applied throughout the operation. Strict compartmentation is maintained throughout NSA and individuals are permitted knowledge only of the specific fields with which they are concerned. In the intelligence community, certain sections are established for the receipt of COMINT and it is the responsibility of these sections to meld COMINT with information from other sources to develop the complete intelligence product. If this product contains information derived only from COMINT, the product retains the COMINT classification, but if COMINT merely corroborates information from other sources, the COMINT classification is not required. This compartmentation and restriction of COMINT to certain specifically cleared individuals constitutes an impediment to the development and use of the complete intelligence product and of ideas, but

TOP SECRET

it appears to be a necessary price to pay for the security of COMINT operations. Among the 4,687 recipients of COMINT are approximately 2,200 members of CIA. A large portion of these are concerned only with plain text traffic. Although these individuals are cleared for COMINT without restrictions, in practice they are given only the plain text traffic with which they are directly concerned. The large number thus cleared for COMINT may, consequently, not be quite as alarming as a first glance would indicate, but it is nevertheless a potential danger to security.

IV RESEARCH AND PLANNING

Research and Development

The tremendous volume of intercept which is received by NSA makes it imperative that maximum use be made of machines to replace or supplement manpower. Great use is being made of International Business Machines in order to select out and bring together information of any particular category. Without such standard machines, the time and labor involved in searching through millions of messages for particular bits of information would be prohibitive. These machines are used routinely in the analytic processes of NSA.

There is also a necessity for electronic computers and analytic machines to do tasks in the field of cryptanalysis in the effort to read encrypted messages. This machine work represents millions of man hours and permits work of a magnitude which would otherwise be utterly impossible. Some of these tasks, which are extremely complicated, can be performed by general-purpose electronic computers, whereas for some tasks, special-purpose computers must be designed, tested, and constructed. NSA now has nine general-purpose and sixteen special-purpose machines,

TOP SECRET

TOP SECRET

which is by far the largest and most comprehensive collection of electronic computers in this country, and, therefore, presumably in the world. Our cryptanalytic effort would collapse without them.

In the development of these electronic "brains," the need is first determined by cryptanalysts attempting to solve a particular system. If a survey of available, existing electronic machines disclosed that there is no machine which can do the desired work, and the problem is of sufficient importance to demand its solution, the Research and Development division is called upon to design a machine. If a general-purpose machine can be designed so that it can do the required task and also other tasks, such a machine will be developed for this particular task. R and D makes use of the entire electronic industry in its development of new electronic machines.

There is also a need for the development of special equipment for the interception of messages as foreign governments put new types of transmissions into use. In this field, R and D works closely with the field test boards of the three Armed Forces.

Up to and including fiscal year 1955, appropriations for R and D of NSA have run between 13 and 14 million dollars. These sums have been adequate to meet the needs. It takes two or three years, or more, from the time the need for a machine becomes known until the machine can be developed and put into use. Because of this time lag, it is imperative that through research and development, aided by the very best talent available and by adequate funds, our development of machines and equipment be kept ahead, insofar as practicable, of the actual needs in order that the final product of NSA may be both timely and adequate. The

TOP SECRET

stantly ahead of its adversaries lest it gradually lose its ability to glean intelligence, which is now of inestimable value, from the field of telecommunications.

Research and development are also conducted in the field of communications security, leading toward a higher degree of security for all telecommunications.

War Plans

War plans are prepared by NSA in conformance with the war plans produced by the JCS; there is close collaboration on the working level^A between NSC plans and policy personnel and the Joint Staff. The three service cryptologic agencies then prepare war plans based upon the NSA plans. The NSA plans take into consideration present capabilities and future requirements. An effort is made to forecast the requirements five and ten years into the future. Subsequent budgetary plans are based upon the current war plan, with adjustments made each year. Plans have been issued to the overseas COMINT commands to effect the transfer of operational control to direct support operations in the event of hostilities.

Alternate Sites

The first echelon of NSA commenced its move from Arlington Hall Station, Virginia, to Fort Meade, Maryland, in January 1955. The second echelon is scheduled to move in June 1955, and the move should be completed by December 1956. The present alternate site for NSA, in the event of disaster, is the University of Maryland, and some communication facilities have been installed there. NSA is now in the process of selecting a more distant site within 75 miles of Washington.

An alternate site for the COMINT communications center in
Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

25X3

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

25X3 [] is now planned for location in [] the communication facilities have not yet been installed. 25X3

V PERSONNEL AND TRAINING

Personnel

The effectiveness of our COMINT efforts depends ultimately upon the support of the Departments of the Army, Navy, and Air Force, and, more specifically, upon the efficiency of the three cryptologic services. Although NSA exercises operational control and provides technical support, the cryptologic services provide the personnel and facilities, conduct the training, and provide logistical support. COMINT starts with the intercept operator, and he is the weakest link in the production chain.

This weakness can be traced to conditions which are not unique to the COMINT area, but here they are especially serious because of the sensitivity and importance of COMINT to the national security. The United States is attempting to maintain a tremendous COMINT effort, with the base of the pyramid comprised largely of relatively inexperienced, semi-skilled operators enlisted or drafted for too short a term really to expect maximum or even acceptable efficiency.

This same weakness extends upward through the noncommissioned and junior officer grades, resulting in a lack of highly-skilled guidance for the semi-skilled operators.

Because personal integrity, sound judgment, and a high degree of technical skill play an abnormally important part in the production of COMINT, the personnel assigned to NSA and the three cryptologic services should be of high quality and should remain in the activity for long periods of service. This refers specifically to the intercept operators,

TOP SECRET

the cryptanalysts, the traffic analysts, and the supervisors and directors of these individuals. Because the work is highly specialized and there is no field of similar nature outside of the COMINT field itself from which personnel may be drawn, all of the personnel are trained after selection for such duty. Consequently, whether an individual is a civilian or member of one of the military services is of secondary importance. Within NSA, one-third of the personnel are drawn in equal numbers from the three military services, and individuals are assigned to duty in accordance with their capabilities and experience and without regard to military or civilian status. The situation within the three military cryptologic services is different in that the personnel are almost entirely military, with civilians limited to duty in continental United States and largely to administrative and maintenance duties. The COMINT effort suffers from a normal turnover in the lower grades of civilian personnel, but especially from the rapid turnover of military personnel. There is a relatively small number of military personnel who have served successive tours of duty in one of the cryptologic services, some of them since before World War II, and these individuals are of great value. Although the military personnel theoretically serve minimum tours of three years with the cryptologic services and the Director, NSA, has the authority to accept or disapprove the selection of officers prior to their assignment to NSA, in practice a considerable number of tours are curtailed for various reasons, including release of individuals from military service. A conspicuous example has occurred in the assignment of Reserve officers to the cryptologic services for their two-year tour of active duty following graduation from ROTC. These officers must be given security clearance, which takes an average of two

TOP SECRET

to four months, and sent to school, lasting about six months, after which they receive on-the-job training. Their productive period of service thus is normally less than one year. This is an extremely wasteful utilization of such personnel. A similar situation exists with regard to enlisted men drafted for two years. Such men who become intercept operators after clearance, training, and shipment overseas usually have about eight months of productive service and they seldom become really expert in their work. The percentage of Regular officers in the cryptologic services is extremely small.

The problems arising out of the instability of service of military personnel are not, of course, limited to the cryptologic services, but those problems are especially acute in these services. The cryptologic services must be given more favorable treatment by the military departments than has been done in recent years. Individuals must be specially selected for this duty and they should be rewarded accordingly.

The relatively more stable period of service of civilians as compared with military personnel has led the Director, NSA, to replace the latter with civilians where practicable. One station, manned only by civilians, has been in operation for several months and is considered one of the better and more successful intercept stations. With the success of that station in mind, the Director, NSA, has recently initiated action whereby the ASA will employ one hundred civilian intercept operators for the purpose of replacing enlisted men in key positions within military fixed stations. This operation will be carefully studied and if it is successful more civilian intercept operators will be employed. It is not remotely possible, however, that all enlisted men in the cryptologic services could be replaced by civilians.

TOP SECRET

Much consideration has been given to developing a larger corps of military COMINT specialists. Prior to World War II, the cryptologic services of the Army and Navy were small. The Army service was composed largely of civilians while the Navy element was largely officers. During the war, these services were greatly expanded with temporary officers and enlisted men, and after the war many of the temporary officers reverted to civilian status but remained in the cryptologic effort and are now employed by NSA. Meanwhile, most of the Regular Navy officers who earlier were in the Navy cryptologic service have since been retired or have been assigned to other duties. The Air Force has no officers with more than a few years' cryptologic experience. At present, nearly all of the officers of each of the services assigned to COMINT duty are Reserve officers and relatively few serve more than one tour of three years on such duty, unless they have signified their desire to be specialists in that field. Of the officers assigned to duty with the cryptologic services, few have volunteered for the duty. In the Army, officers of all the combat arms and of some of the technical services in addition to the Signal Corps have been assigned to COMINT duty. Relatively few enlisted men serve more than one tour of duty with the cryptologic services.

It is neither necessary nor desirable that all of the military personnel on COMINT duty be career specialists in that field or that they be communications specialists. It is extremely desirable, however, that those who are selected for this duty be more carefully selected than has sometimes been the case, that a larger percentage than at present be COMINT specialists, that some of them also have been communications specialists, and that a larger portion be Regular officers in

TOP SECRET

order that there may be a flow of high quality, experienced officers to the senior positions within the organization. Unless this last step be taken, civilians will inevitably become the only individuals qualified to fill the top positions. In the development of military COMINT specialists, care must be exercised not to retard their promotion in comparison with other outstanding officers. Some interchange in tours of duty between COMINT and intelligence specialists would be desirable.

The more senior of the relatively few officers who have served more or less continuously in COMINT duties over long periods of years, dating back to before World War II, are now approaching retirement. Some of these officers could be of great value to NSA because of their long experience and expert knowledge of COMINT matters. The Act of July 31, 1894, however, is an effective bar, through limitation imposed on their pay, to employment by NSA of such officers after their retirement. It is emphasized that there is no related field from which COMINT experts can be drawn; the military cryptologic services and NSA are the only organizations wherein such specialists are trained and developed. The number of COMINT experts is far less than are needed today and doubtless this situation will continue for years to come. Attention is invited to the fact that special legislation (Public Law 53, 82d Congress, June 26, 1951) authorizes the employment, without loss of pay, of not more than fifteen retired officers or warrant officers by the Central Intelligence Agency. Since the field from which COMINT experts or specialists can be drawn is much narrower than the field from which intelligence personnel can be obtained, there is even greater need for special authorization for NSA than for CIA.

TOP SECRET

The selection, training, and job classifications of NSA civilian personnel are affected by the Civil Service Commission rules and regulations. In order to help maintain the necessary secrecy surrounding NSA operations, all NSA civilian personnel are placed under Schedule A. This classification gives the Director, NSA, authority to employ personnel without regard to civil service eligibility lists, to discharge them for cause, to transfer them from one job to another, and to put them in a grade structure on a par with civil service grades. Schedule A is of great benefit to NSA, but does not completely solve the personnel or security problems because NSA is required to report to the Civil Service Commission each time an individual is employed, discharged, or reclassified within NSA. Such reports could result in a breach of security in that it would be possible for a person who has access to the civil service records to compute the number of persons employed by NSA and to gain some knowledge of the types of jobs within NSA. Furthermore, it is difficult to fit many of the jobs at NSA into the civil service job structure, although this problem appears to have been satisfactorily solved through mutual cooperation between NSA and the Civil Service Commission.

Because of the large number of very competent and highly educated individuals required by NSA, and in order to retain a high percentage of them in the face of attractive opportunities to transfer to private industry, NSA needs a relatively large number of "super grades" or similar pay grades. Schedule A does not solve this problem, and NSA has found itself in an awkward position in this respect since neither the Department of Defense nor the Civil Service Commission has assumed full responsibility for the agency's personnel needs. The agency is

TOP SECRET

now allocated 23 super grades (two Grade 18's, two Grade 17's, and nineteen Grade 16's) obtained partly from the Department of Defense and partly from the Civil Service Commission. This number probably is adequate for the moment. Eleven of these positions, however, are authorized under the Defense Production Act of 1950 which expires June 30, 1955, and NSA is, therefore, now faced with the probable reduction to twelve super grades. The Director, NSA, desires that he be authorized, for future use, a total of fifty super grades and fifty positions under Public Law 313, in order to provide a properly balanced grade structure for the highly skilled scientific and technical personnel of NSA. Public Law 313 authorizes payment of salaries between \$10,000 and \$15,000 to designated scientific and technical personnel without raise in grade. This matter should be given careful consideration by the Department of Defense.

Another situation which affects the civilian personnel relates to foreign service. Approximately NSA civilians now serve overseas, and that number is expected to increase. The Director, NSA, cannot order a civilian overseas unless he volunteers for such assignment. Although NSA civilians often serve in proximity to U. S. military personnel or civilian employees of other governmental agencies or departments, they frequently find themselves at a disadvantage with respect to privileges or "fringe benefits," such as commissary or "PX" privileges, quarters, medical care, transportation of automobile overseas, or leave credits enjoyed by State Department employees or military personnel in the same area. NSA civilians should be extended the same privileges as CIA personnel under similar circumstances.

25X3

competent scientists to serve as consultants in the solution of some of its technical problems. The agency's experience with consultants has not been entirely successful, especially when the consultants were employed for only a few days at a time. The Atomic Energy Commission has employed scientific consultants at a daily pay rate, in some instances, as high as \$100, whereas NSA pay rates may not exceed \$50. This fact alone may not account for the AEC's more successful use of consultants, but it probably is a factor.

Both the AEC and CIA are exempted by law from civil service regulations which are applicable to NSA, although the three agencies are faced with similar personnel problems. There is no specific statutory authorization for NSA; it was created by National Security Council Intelligence Directive No. 9. Although NSA doubtless would benefit from a statutory charter, the seeking of legislation for this purpose does not appear to be necessary at this time. Further effort should first be made to solve the personnel problems of NSA through the Department of Defense.

Initial examination of the NSA organization suggests that there are too many individuals in administrative positions. Further examination, however, does not sustain that initial impression when weight is given to the fact that NSA exercises operational control over intercept stations and processing to such a degree that it considers the operations of each position and requires detailed knowledge of all operations, including the number of operators available. In some respects, this situation may be compared with a division commander controlling the operations of each infantry company and artillery battery. Obviously, NSA plans must be prepared in great detail. Only a detailed personnel survey of

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
excessive number of individuals actually are engaged in administration.

The requirement that all security clearances be completed before NSA employees are permitted to work within the restricted areas necessarily affects the economical and efficient utilization of newly employed personnel. The average time required for clearance is two to four months. Prospective employees are given a polygraph test as a first step in their employment and those who pass that test are then given a temporary confidential clearance which permits them to pursue the NSA basic course of instruction and indoctrination, which lasts four weeks. During the remainder of the period while awaiting full clearance, these new employees are kept at the school and are engaged in clerical or administrative work which does not involve classified information. Enough of such work can usually be found to keep a new employee occupied for a month after completing his course; beyond that period, however, his time is not profitably used. Clearances sometimes seem to be unduly delayed and one instance was noted where a student was retained at the school eighteen months while awaiting clearance. Since NSA does not control the obtaining of clearances, the time consumed while awaiting clearance is a phase of the major problem of obtaining prompt clearance for all civil service employees who require security clearance.

Tables showing the strength of the four cryptologic agencies are summarized below:

	Estimated June 30, 1954	Estimated June 30, 1955	Projected June 30, 1956
NSA			
ASA			
NSG			
AFSS			
Total			

25X3

These figures show that between June 30, 1954, and June 30, 1955 there will be an overall increase of [] persons connected with COMINT operations if the authorized strengths are fulfilled, or a net gain during that period of approximately five percent. Between June 30, 1955 and June 30, 1956, there will be a similar increase of [] persons, or thirteen percent above the 1955 level.

25X3

25X3

Schools and Training Activities

Training is conducted by NSA and each of the three cryptologic services. The Director, NSA, is responsible for the establishment of minimum standards which govern the training conducted by the three services, but he does not conduct inspections of their schools and he does not have specific authority to do so. Each of those services maintains a school wherein training is conducted primarily for intercept operators and, to a lesser degree, for cryptanalysts. The Army also conducts a school for training in languages, but this school is not used exclusively by the cryptologic services. In view of the fact that intercept operations are conducted by units of the three cryptologic services and, consequently, those services determine to some extent their methods of operation and the equipment which they use, it appears to be reasonable that separate schools be maintained for each of the services. Although most of the intercept operations are conducted from land stations, the Navy does conduct some from on board ship and the Air Force some from planes in flight. Consequently, there is some need for minor variations in training. The largest of the three schools is the one conducted by the Army and it operates at capacity level. Inquiry into this matter has not disclosed that any increase in efficiency or economy could be effected through combining the three schools into one school, or

through integrating the separate schools into one unified school system.

In addition to the schools conducted by the three services, NSA also conducts a school for the orientation and indoctrination of all employees, military and civilian, and for the cryptologic training, languages (intercepts are made in approximately forty-three languages), clerical and management training. From time to time, NSA conducts special courses for a particular purpose, and one such course is now being conducted for radio-telephone intercept operators. This course is being conducted as a pilot model and instructors from the Army are now being trained to the end that this course will be transferred to the Army school in the near future. Among various special courses conducted in the NSA school is one for rapid reading for the purpose of training employees whose duties require that they scan a large volume of messages.

The special language courses conducted by NSA are more economical than would be the use of general language schools because they are pointed toward the specific objective established by the intercept problem. In these language courses, effort is not made to teach the student to speak the language, but only to grasp so much of it as is necessary for a particular task. Courses are also conducted in certain languages which are not generally taught in the United States, such as Amharic. NSA has availed itself of personnel within the diplomatic community or elsewhere living in Washington to assist in conducting some of these rare courses. Recently, to cite one example, there has been a need for many more linguists in Vietnamese than are available for employment.

In addition to the full-time language courses conducted in the NSA
Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

school, short-time courses are also conducted in the Office of Production of NSA, which students attend for one hour at a time in conjunction with their normal work in order to gain greater proficiency in the language with which they are working.

It is obvious that the COMINT effort of NSA and the three cryptologic services suffers from the general, overall shortage of linguists both in the military services and in civil life. From a long-range viewpoint, the services would benefit immeasurably if fluency in one or more foreign languages were made a requirement for graduation from high schools and colleges, and if the Armed Forces placed greater emphasis on that requirement. For example, a large fraction of the Armed Forces are now serving overseas. If those individuals were required to acquire a high degree of fluency in the language of the country in which they serve, we would in time build up a linguistic reservoir of tremendous potential value. This is merely mentioned as part of a much broader subject than communications intelligence.

The management courses are conducted for the specific purposes of training individuals to fill supervisory positions within NSA. The basic course of instruction and indoctrination conducted by NSA for all new employees lasts four weeks. Following that basic course, selected students undergo further instruction or training, depending upon the particular job which they have been selected to fill.

During fiscal year 1954, a total of 809 persons studied languages in the NSA school. In addition to the students in attendance at the NSA school, provision has been made to permit selected career employees to attend universities on scholarships and fellowships in order to achieve advanced training and thus increase their proficiency and value to NSA.

Selected civilians of NSA also attend the National War College and the Industrial College of the Armed Forces.

The total number of students of NSA and the three cryptologic services who attended courses in 1954 follows:

	Completed in 1954	Commenced in 1954, to be completed in 1955
Army		
Navy		
Air Force		
NSA		
Total		

25X3

The courses conducted by NSA do not duplicate those conducted by the three cryptologic services, and either are not available elsewhere or are not available in such form as to suit the needs of NSA. The schools appear to be well conducted.

VI LOGISTICS

The National Security Agency budgets for civilian personnel, supplies, materials, equipment, and some other requirements (such as part of the cost of courier service) required in direct support of the agency. Most administrative requirements are budgeted by the security services of the three military departments and military personnel are paid by their respective departments.

The budgets of the three cryptologic services are all handled differently, and it is, therefore, difficult to make direct comparisons between the budgetary data of those services. The Army Security Agency budgets for civilian personnel, supplies, materials, and equipment in direct support of its cryptologic mission, but other requirements, including administration, communications, and pay of military personnel

TOP SECRET

are budgeted by other elements of the Army. The Navy Security Group likewise budgets for civilian personnel, supplies, materials, and equipment in direct support of its cryptologic mission, but other requirements, including logistical support of the cryptologic units, administration, and communications are budgeted by other Navy elements. For example of differences between the Army and Navy, Army cryptologic units are to some extent self sufficient with their own overhead and support units, while Navy cryptologic units are normally attached to other Navy units which furnish the overhead and logistical support. The Air Force Security Group budgets for a higher degree of its operations and support, including its communications and administrative requirements as well as civilian personnel, supplies, materials, and equipment; it does not budget for pay of military personnel.

The total appropriations for the cryptologic services for fiscal years 1953, 1954, and 1955, and the estimated appropriations for fiscal year 1956 follow:

	Fiscal Year 1953	Fiscal Year 1954	Fiscal Year 1955	Fiscal Year 1956	25X3
NSA					
AFSS					
NSG					
ASA					
Total					

The appropriations for NSA, which are distinct from ASA, are all included in the Army budget, but are concealed therein for security reasons.

Almost half of the expenditures of NSA are for its civilian payroll. In view of the different accounting practices of the four agencies con-

TOP SECRET

TOP SECRET

earned and because of the fact that many of the costs are merged in other appropriations, it is extremely difficult to determine the actual total cost of the COMINT effort of the Government. Estimates of NSA conclude that in the neighborhood of [] are expended annually on the COMINT effort. This estimate includes the cost of military and civilian personnel, transportation, communications, equipment, and maintenances.

25X3

The comptroller of NSA operates directly under the chief of staff. The comptroller prepares the budget and also conducts scheduled manpower surveys to insure economical and equitable utilization of personnel.

VII ELECTRONICS INTELLIGENCE

Electronics intelligence, commonly known as ELINT, has not been exactly defined to the satisfaction of all who are concerned with it. For the purposes of this survey, however, it is defined to include all electronic emissions other than those which convey messages, ideas, or pictures. In the electronic field, emissions of ELINT merge into and overlap to a small degree the emissions of COMINT. ELINT covers a wide range of weapons, including radar, [] etc. The study of ELINT is in its infancy and only future experiments can determine the extent of this electronics field.

25X1

At the present time, direction over the ELINT operations of the Army and Navy is rather loosely controlled through a small, combined agency called Army-Navy Electronics Evaluation Group (ANEEG) which is co-located with but entirely separate from the Naval Security Group, together with part of NSA, on Nebraska Avenue, NW, Washington, D.C. The

TOP SECRET

25X1

interception of ELINT emissions is carried on separately by the Army and Navy; ANEEG is concerned with the identification, analysis, evaluation, and interpretation of the electronic interceptions. The Air Force ELINT operations are entirely separate; ELINT emissions are intercepted by the Air Force Security Service (AFSS) with headquarters at Kelley Air Force Base at San Antonio, Texas, and are directed and evaluated by the Air Force Technical Intelligence Center (ATIC) at Wright-Patterson Air Force Base, Dayton, Ohio. Some coordination of ideas and knowledge is obtained among Army, Navy, and Air Force ELINT activities through a working group of the Joint Technical Intelligence Subcommittee, Joint Intelligence Group, of the Joint Staff, but that subcommittee does not effect operational control. Some coordination is also achieved through direct contact and the interchange of information of the ELINT organizations of the three services. [] is also engaged in the interception, analysis, and evaluation of ELINT; there is limited coordination between [] and the military services in this field.

There has been discussion among the Armed Forces and the Defense Department for at least eighteen months regarding possible joining together, in some form, of ELINT activities of the three armed services. In these discussions, the interest of CIA in ELINT seems to have been largely, if not entirely, ignored, although CIA appears to have a genuine direct interest in ELINT operations. The Office of Special Operations, Department of Defense, has prepared a plan, which was eventually concurred in by the three military departments and the Joint Chiefs of Staff, "to consolidate ELINT analysis activities under a single direction, to guide and coordinate the collection of all ELINT information and to provide for optimum interaction and mutual support between ELINT and

TOP SECRET

COMINT." This plan makes the Secretary of one of the military departments, presumably the Air Force, executive agent for the Secretary of Defense. The plan contemplates implementation through a National Security Council Intelligence Directive. It has not at this writing been approved by the Secretary of Defense.

There is some relationship between ELINT and COMINT in that it cannot always be readily determined whether a given electronic intercept is ELINT or COMINT; COMINT is of value in interpreting some ELINT and vice versa; and intercept positions for the two are sometimes advantageously co-located. For example, Air Force Security Service positions in the [redacted] have been effecting interception of ELINT and COMINT. Under standing instructions, the ELINT intercept is to be sent to ATIC through AFSS channels and the COMINT intercept is to be sent direct to NSA. The intercept positions requested authority to turn the COMINT intercept over to a unit in the [redacted] and they were authorized to turn it over to the Air Force COMINT group headquarters [redacted]. It was then learned that COMINT and ELINT intercept were so intermingled on the same tape recordings that it was impracticable to separate them. In another instance, ELINT intercept positions initially made little progress on their mission regarding [redacted]. When COMINT intercept positions were co-located with them, the interchange of information at the site brought about definite improvement in the ELINT interception.

The ELINT operations of the countries of [redacted] are completely integrated with their COMINT operations. [redacted] in particular with complete integration, are reported to have achieved better results in ELINT than has [redacted].

TOP SECRET

to weapons systems and because relatively little is understood about ELINT and its capabilities at this time, it seems reasonable that the interception of ELINT emissions should not be under as high a degree of centralized control as is now established for COMINT. However, the study, analysis, evaluation, interpretation, and research and development of ELINT should be under central direction in order to bring about the maximum use of ELINT products.

There must be an operating body with executive authority, but its composition and degree of authority have created a wide divergence of opinion. As noted above, one proposal is to charge one of the military departments with this responsibility. Other solutions which have been suggested are to create an agency for this purpose (possibly through conversion and enlargement of ANEEG), or to utilize an already functioning agency by giving it ELINT as an additional responsibility. The only agency seriously considered for the latter purpose is NSA. The objections to a new agency which would be separate from and coequal with NSA, including ANEEG, are the lack of complete coordination in such a solution between COMINT and ELINT, except through USCIB in policy matters, and the lack of economy in personnel and funds which would be inherent in the creation of a new agency. Lack of consideration of CIA is an added objection to the specific plans proposed. The objections to charging NSA with additional responsibility for ELINT stem from the fear that ELINT, being a much smaller activity, would not receive adequate attention from the Director, NSA, and his staff, who already are fully occupied in the direction of a very large agency. There also is the fear of the military departments that their interests would not be fully met by an essentially civilian agency such as NSA. They have a similar fear

TOP SECRET

of policy control over ELINT by USCIB.

The following considerations with regard to NSA are deemed important. It now comprises three major divisions - security (COMSEC), production (COMINT), and research and development. If a fourth division, ELINT, were added, it would require far less augmentation to the already operating staff and R and D of NSA than would be required for the overhead of a completely separate ELINT agency. Furthermore, NSA has demonstrated a responsiveness to the COMINT requirements of the military departments and should likewise be expected to give full support to their ELINT requirements as well as the ELINT requirements of CIA. The requirements of CIA certainly must not be overlooked; they do, however, require clear definition. Although responsibility for ELINT would unquestionably impose another heavy burden on the Director, NSA, and his staff, it is believed that ELINT would not suffer from lack of attention. NSA has now been in operation long enough so that the multitudinous problems of a new organization have begun to diminish in number and magnitude. On the other hand, the experience of NSA in the creation of that national agency would be of inestimable value in bringing a related member of the electronics community into a coordinated national effort.

Although it is believed that ELINT intercept operations should not, at the present stage of development, be as fully integrated as are the current COMINT intercept operations, it is impracticable in a survey of this nature to determine and delineate the exact degree of integration or decentralization of intercept operations.

15
TOP SECRET

TOP SECRET

VIII RECOMMENDATIONS

The National Security Agency is basically well conceived, well organized, and efficiently operated. Much credit must be given to its Director, whose intense interest and outstanding ability have greatly contributed to the operation. Although attempts to discern USSR intentions unfortunately have not been successful, COMINT contribution to the intelligence effort has enabled those responsible to better estimate probable courses of enemy action, has greatly assisted in our negotiations of agreements with other nations, and has provided military commanders with intelligence not otherwise obtainable.

There is need for further ^{expansion} expansion of the COMINT effort and economy motives alone should not result in curtailing this means of insurance during an era when not only our national security but our national survival as well may depend on adequate intelligence.

The present organization, wherein the Director, NSA, has delegated operational control and responsibility for processing the intercept in some instances to a major cryptologic organization and in which he contemplates further decentralization as rapidly as the cryptologic elements in the field are sufficiently trained and equipped, is sound in concept and should be continued.

Recommendation No. 1

THAT THE NATIONAL SECURITY COUNCIL DIRECT USCIB TO ESTABLISH COMINT REQUIREMENTS IN THE LIGHT OF COMINT REALITIES AND CONSIDERATION OF CAPABILITIES OF OTHER INTELLIGENCE SOURCES. THIS OPERATIONAL GUIDANCE TO NSA SHOULD BE SO CLEAR AND SUGGEST AS TO REQUIRE MINIMUM INTERPRETATION BY THE DIRECTOR, NSA, OF WHAT IS REQUIRED AND ITS DEGREE OF

TOP SECRET

IMPORTANCE. USCIB SHOULD BE PRIMARILY CONCERNED WITH END PRODUCTS AND THE DIRECTOR, NSA; SHOULD DETERMINE THE BEST WAY OF PRODUCING THE END PRODUCT. IF USCIB FAILS AFTER A REASONABLE LENGTH OF TIME TO PROVIDE MORE ADEQUATE GUIDANCE TO THE DIRECTOR, NSA, THEN THE LATTER SHOULD BE MADE A MEMBER OF THE INTELLIGENCE ADVISORY COMMITTEE.

NSA is a collector of intelligence and in some respects a producer as well. The Director of NSA has not received the guidance which he must have from USCIB to make his product most useful. USCIB has not identified intelligence requirements which can be best filled by COMINT and has taken little notice of the capabilities or limitations of NSA. The Director, NSA, needs to know what is important and what is less important, but the comprehensive lists of requirements established by USCIB fail to make sufficient differentiation. Thus, the Director, NSA, is required to weigh one commitment against another, decide on a priority, and program accordingly. He has not sought this responsibility, but rather, lacking adequate guidance, has been forced to assume it. His task is made even more difficult because, not being a member of the Intelligence Advisory Committee, he feels sealed off from the deliberations which ultimately result in establishing intelligence requirements. He believes that, since sufficient guidance is not forthcoming from USCIB, a partial remedy, at least, would be NSA membership on the IAC. The task force does not believe at this time that the remedy is NSA membership on the Intelligence Advisory Committee. It feels, rather, that proper direction can be attained through revision of present USCIB procedures to secure realistic COMINT objectives and priorities from the intelligence objectives formulated by the IAC. USCIB procedures should be designed to produce results rather than being concerned with

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

implementation. USCIB should also look to the Director, NSA, for advice with respect to the effect of requirements levied on NSA technical operations. Technical considerations involved in the NSA operation should not become paramount in the production of intelligence, and, therefore, the task force believes that the present composition of USCIB membership should remain substantially the same rather than including communications or other specialists, although there is no objection to establishing appropriate subcommittees to advise USCIB with respect to technical matters. (Pages 5-9)

Recommendation No. 2

THAT THE DIRECTOR, NSA, BE GIVEN CLEARCUT DIRECTIVES WHICH WILL ENABLE HIM TO MAKE MUCH GREATER AND CONTINUING EFFORT TO PRODUCE HIGH-LEVEL COMMUNICATIONS INTELLIGENCE. THIS IS OF SUCH GREAT IMPORTANCE THAT MONETARY CONSIDERATIONS SHOULD BE WAIVED AND AN EFFORT AT LEAST EQUAL TO THE MANHATTAN PROJECT SHOULD BE EXERTED AT ONCE.

NSA has not produced the amount of high-level COMINT concerning the Communist orbit which is desired by the intelligence community. The COMINT effort should be directed primarily to tasks for which it has a unique capability and NSA should not be asked to produce information of marginal value or to duplicate unnecessarily information which can be collected through less critical sources. In this respect, a major difficulty stems from the intelligence agencies' unwillingness to accept less day-to-day intelligence and their insistence that NSA commit its efforts on those phases of COMINT which are immediately productive. The Director, NSA, has an insufficient number of capable personnel for a maximum and continuous effort on long-range cryptanalysis if he attempts to satisfy all requirements. Furthermore, he is unable to allocate enough intercept positions for

operation against the more important foreign traffic and at the same time fulfill all other requirements. Another important consideration is that the principal limitation is not in money or machines, but rather in human brains. All possible approaches to this problem must be explored with the objective of [REDACTED]

25X1

[REDACTED] This is a primary objective and must be pursued even though it might result in some reduction in the production of [REDACTED] (Page 18)

25X1

Recommendation No. 3

THAT ELINT AND COMINT BE INTEGRATED TO THE EXTENT OF PLACING ELINT UNDER NSA FOR ANALYSIS OF THE PRODUCT AND GUIDANCE AND COORDINATION IN THE COLLECTION AND DISSEMINATION OF ELINT. THE AUTHORITY OF OPERATIONAL COMMANDERS OVER THEIR INTEGRAL ELINT RESOURCES, HOWEVER, SHOULD NOT BE ABRIDGED. USCIB OR THE COMBINED BOARD WHICH IS RECOMMENDED IN THIS REPORT TO REPLACE IT SHOULD EXERCISE ONLY POLICY CONTROL OVER ELINT MATTERS.

The present separation of ELINT from COMINT and the division of operations between the Army-Navy Electronics Evaluation Group (ANEEG) and the Air Force in the ELINT field cannot be justified where national intelligence is concerned. The inherent relationship between COMINT and ELINT has been recognized by every non-Communist country engaged in the collection of ELINT except the United States, and experience to date demonstrates that an integration of the analysis of COMINT and ELINT produces better results. National and departmental interests will be better served, and a more economical and efficient operation will result, if ELINT is placed under NSA for analysis of the product and guidance and coordination in the collection and dissemination of ELINT.

TOP SECRET

At the same time, the direct interest of each of the military services in the product of ELINT must be recognized. There is a considerable amount of ELINT which does not require laboratory or "rear echelon" analysis in order to be immediately valuable to the military commander in the area where the interception is made. No system of centralized control of analysis or collection should, therefore, be permitted to delay the receipt of such ELINT by the commander concerned. The authority of operational commanders over their integral ELINT resources should not be abridged. (Pages 41-45)

Recommendation No. 4

NSRFB ✓

THAT THE MILITARY SERVICES AND NSA CONTINUE TO STRIVE FOR A HIGHER DEGREE OF CRYPTOGRAPHIC SECURITY; THAT THE PROBLEM OF COMMUNICATIONS SECURITY, INCLUDING PLAIN TEXT MESSAGES AND TRAFFIC ANALYSIS OF ENCRYPTED MESSAGES, BE RESTUDIED BY USCSB (OR THE COMBINED BOARD AS RECOMMENDED IN THIS REPORT) WITH A VIEW TOWARD REDUCING TO THE LOWEST PRACTICABLE LEVEL THE QUANTITY OF INFORMATION RELEASED THROUGH TELECOMMUNICATIONS; AND THAT NSC 168 BE REEXAMINED TO ASCERTAIN IF THE DIRECTOR, NSA, HAS SUFFICIENT AUTHORITY TO CARRY OUT HIS COMSEC RESPONSIBILITIES.

The cryptographic systems used by the military and civil elements of the Federal Government afford adequate security when properly used. The number of probable compromises of encrypted messages, although a very small percentage of the total number of encrypted messages, is sufficient to permit the possible acquisition of intelligence by a foreign power. A much greater source of intelligence is available to a foreign power through interception of a large number of plain text messages originated by military and civil interests, and traffic analysis of encrypted messages. (Pages 19-22)

TOP SECRET

Recommendation No. 5

THAT A SINGLE BOARD WITH APPROPRIATE TECHNICAL SUBCOMMITTEES HAVE POLICY COGNIZANCE OVER COMMUNICATIONS INTELLIGENCE AND COMMUNICATIONS SECURITY. IF THE RECOMMENDATION TO PLACE THE EVALUATION AND ANALYSIS OF ELINT UNDER NSA IS ADOPTED, THEN POLICY GUIDANCE FOR ELINT AS WELL AS COMINT AND COMSEC SHOULD BE EXERCISED BY THE PROPOSED SINGLE BOARD.

The desirability of the present separation of policy guidance concerning communications intelligence and communications security through two boards is questionable since both functions are related aspects of telecommunications. A single board having policy cognizance over communications intelligence, communications security, and electronics intelligence (ELINT) would provide improved coordination and better direction of NSA and would also insure that each of these functions receives proper emphasis and attention. Because the whole intelligence and communications security operations are so intimately related to the communications-electronics field, it would be essential that appropriate subcommittees composed of technically and operationally qualified personnel be established to advise the board. Both USCIB and USCSB are substantially comprised of the same agency membership, although USCSB also includes AEC and Treasury. These latter agencies, however, do not have as substantial interest as the other departments and their interest probably would be just as well served through membership on supporting committees. (Pages 5-9, 19-22)

Recommendation No. 6

THAT THE DEPARTMENT OF DEFENSE CAREFULLY STUDY THE ORGANIZATIONAL STRUCTURE AND PROPER POSITIONING WITHIN ITS RESPECTIVE SERVICES OF THE

TOP SECRET

TOP SECRET

THREE CRYPTOLOGIC AGENCIES - AFSS, ASA, AND NSG - WITH A VIEW TOWARD IMPROVING THEIR PRESTIGE AND EFFECTIVENESS, THEREBY STRENGTHENING THEIR PERSONNEL ASSIGNMENT POLICIES AND LOGISTICAL SUPPORT.

The success or failure of the COMINT operation ultimately rests with the cryptologic services of the Army, Navy, and Air Force. For this reason alone, the organizational structure and proper positioning of the ASA, NSG, and AFSS within their respective services deserve careful study. Moreover, in order to do an adequate job, the cryptologic services must be in a position properly to recruit, train, and reward personnel who intend to make COMINT a career. This they cannot be expected to do if they are forced to compete with other branches of the service without having "top-level" appreciation and support. Currently, the organizational structure and positioning of the Air Force Security Service seems most nearly to meet these qualifications, while the status of the Navy Security Group, with a divided subordination, appears least conducive to effective operation. (Page 14)

Recommendation No. 7

✓

THAT THE MILITARY SERVICES GIVE GREATER ATTENTION TO SELECTING OFFICERS FOR COMINT DUTIES, ASSIGN REGULAR OR "CAREER" RESERVE OFFICERS TO THE MAXIMUM EXTENT POSSIBLE, INDOCTRINATE OFFICERS IN COMINT PRIOR TO SENDING THEM TO COMMAND FIELD STATIONS, AND ESTABLISH CAREER OPPORTUNITIES FOR SPECIALISTS EQUAL TO THOSE OF THE LINE OR GENERAL SERVICE OFFICERS. ROTATION AND REPLACEMENT PROCEDURES SHOULD BE IMPROVED. THE FEASIBILITY OF USING CIVILIAN INTERCEPT OPERATORS SHOULD BE THOROUGHLY TESTED.

IT IS ALSO RECOMMENDED THAT THE CONGRESS ENACT LEGISLATION TO AUTHORIZE THE NATIONAL SECURITY AGENCY TO EMPLOY SPECIALLY QUALIFIED RETIRED MILITARY

PERSONNEL AS PRESENTLY AUTHORIZED THE CENTRAL INTELLIGENCE AGENCY AND WITH NO RESTRICTION ON THE NUMBER SO EMPLOYED. SUCH LEGISLATION SHOULD ALSO PERMIT THE SECRETARY OF DEFENSE TO RECALL RETIRED OFFICERS TO ACTIVE DUTY WITH NSA AND HAVE THOSE OFFICERS COUNTED AGAINST THE AUTHORIZED STRENGTH OF NSA BUT NOT OF THE RESPECTIVE MILITARY SERVICES.

A disservice is done to the COMINT effort by assigning officers who do not have an aptitude or interest in this field; by assigning Reserve officers who do not intend to serve on active duty any longer than required; by sending officers to command field stations without first training and indoctrinating them in COMINT; by not giving equal career opportunities to specialists; and, lastly, by not properly or more fully utilizing retired personnel with long experience in the cryptologic service.

In the field, the two big problems are rotation and the low reenlistment rate which cause not only breaks in continuity, but varying levels of efficiency. Administrative procedures should be devised which would reduce the instability and consequently lessened effectiveness. For example, in one station there have been at least three almost complete turnovers of personnel during a three-year period. In addition, the time lag between detachment and replacement should be appreciably decreased. The weakest link in the COMINT chain is the intercept operator, due to the rapid rate of turnover.

Although the enlisted intercept operator is doing an inadequate job, the proposed alternative to replace him with a civilian operator has only a limited potential; moreover, it is likely that many of the conditions which make it difficult to make COMINT an attractive career

TOP SECRET

for military personnel will not be solved through employing civilians. Possibly the best solution is to employ a sufficient number of experienced civilians at the working level to provide guidance and establish standards for enlisted operators by working alongside them at stations which require bolstering. The pilot operation for employment of one hundred civilian operators, which was recently initiated by the ASA under NSA guidance, should be continued and carefully studied.

(Pages 27-31)

Recommendation No. 8

✓

THAT THE SECRETARY OF DEFENSE GIVE FURTHER CONSIDERATION TO THE ALLOCATION OF AN APPROPRIATE NUMBER OF "SUPER GRADES" AND POSITIONS UNDER PUBLIC LAW 313 TO NSA; TO THE POSSIBILITY OF FURTHER INDUCEMENTS OR HIGHER PAY TO SELECTED CONSULTANTS; AND TO PRIVILEGES EXTENDED TO CIVILIANS OVERSEAS.

The caliber of civilians working for NSA is generally excellent, particularly those in the professional categories. All of NSA civilian employees are placed in Schedule A. Although this does not in itself solve all of the administrative problems created by the security restrictions which necessarily surround NSA, it creates a generally satisfactory situation, except with regard to the allocation of "super grades" and positions under Public Law 313 which NSA should have. Neither the Department of Defense nor the Civil Service Commission has assumed full responsibility for the allocation of such grades to NSA, but each has allocated some super grades. NSA is in a less advantageous position than the Atomic Energy Commission in the employment of scientific consultants, since the latter agency is able to give them higher pay. NSA civilian personnel who are stationed overseas should, in general, enjoy

the same privileges, or "fringe benefits," as Central Intelligence Agency or other government employees in the same area. (Pages 32-34)

Recommendation No. 9

THAT USCIB OR ITS SUCCESSOR BOARD CLARIFY THE OBJECTIVES AND FUNCTIONS OF INTELLIGENCE LIAISON DETACHMENTS WITH NSA, ESTABLISH UNIFORM PROCEDURES TO BE FOLLOWED BY SUCH DETACHMENTS IN THEIR RELATIONSHIP WITH THAT AGENCY, AND SPECIFY MAXIMUM NUMBERS OF PERSONNEL TO BE ASSIGNED FOR LIAISON DUTIES AFTER EXAMINING THE EXTENT OF INTEREST OF EACH DEPARTMENT OR AGENCY CONCERNED. INTELLIGENCE PERSONNEL ASSIGNED TO LIAISON DUTY WITH NSA SHOULD BE REQUIRED TO ATTEND AN INDOCTRINATION COURSE CONDUCTED BY NSA.

Each of the principal recipients of COMINT, i.e., the intelligence organizations of the State, Army, Navy, and Air Force Departments and CIA, maintains a liaison detachment with NSA. These detachments, particularly those of the three military services, have grown into large operating organizations and a better understanding of the proper relationship between these groups and NSA is needed. Current frictions at the working levels of NSA and the liaison detachments stem largely from misunderstandings which in turn are attributable somewhat to compartmentation, but more to ignorance of the respective needs and problems of NSA and the intelligence agencies.

Personnel assigned to liaison duty at NSA should not only be highly experienced and informed in intelligence techniques, but should have an appreciation of COMINT techniques as well. This can be accomplished and a better relationship established if it were made mandatory for those selected for liaison duty to attend an indoctrination course conducted by the NSA. In addition, USCIB should, after study, define the functions

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

expected to be performed by liaison detachments and the purposes for which those detachments are established. The numbers of personnel assigned to liaison detachments at NSA appeared to be excessive in some instances and probably could be reduced following clarification of the mission and description of duties. (Pages 15-17)

Recommendation No. 10

THAT NSA AND THE THREE CRYPTOLOGIC SERVICES GIVE GREATER EMPHASIS TO, AND CONTINUE TO DEVELOP MUTUAL COOPERATION IN, IMPROVING THE TECHNICAL FEATURES OF INTERCEPT STATIONS.

In order to attain maximum efficiency in communications intercept, greater consideration should be given to engineering and technical aspects of stations. Although the problem is recognized by NSA and the cryptologic services, unilateral actions to influence both station locations and layouts have evidently been handicapped by insufficient appreciation or understanding of some requirements by headquarters and field commands, especially in the earlier years of development. NSA has only comparatively recently given consideration to these phases of COMINT. NSA should step up its efforts in this field, in cooperation with the cryptologic services. (Page 13)

Recommendation No. 11

THAT MORE THOROUGH PERIODIC REINVESTIGATIONS OF PERSONNEL BE MADE. PARTICULAR EFFORT SHOULD BE CONCENTRATED ON PERSONS OCCUPYING THE MORE SENSITIVE POSITIONS.

The security procedures followed by NSA are adequate with the exception of periodic reinvestigations to determine if persons previously certified as having clear records have not in the interim become security risks. The security records, including a National Agency Check, are

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

TOP SECRET

reviewed at five-year intervals, but complete field reinvestigations have not been made at such intervals. Many of those employed by NSA are engaged in rudimentary tasks which, together with the compartmentation that is the rule, would prevent them from seriously compromising the effort. In the highest echelons, a much greater knowledge of the COMINT operation is required and people occupying these positions, consequently, would be able to greatly injure our national security in the event they became security risks. In the task of checking all personnel every few years, the solution might be to establish which positions are the most sensitive and give first priority to the recheck of persons occupying such positions, with lower priority to those in less sensitive positions.

(Pages 22-24)

Recommendation No. 12

THAT THE DIRECTOR, NSA, BE GIVEN AUTHORITY TO INSPECT THE SERVICE CRYPTOLOGIC SCHOOLS AND MAKE APPROPRIATE RECOMMENDATIONS FOR IMPROVEMENT WHERE COMINT IS AFFECTED. ✓

The Director, NSA, has placed great emphasis on education and training of NSA employees. The curriculum at the NSA school is oriented toward COMINT and does not duplicate courses conducted by the military services. NSA does not conduct inspections of the cryptologic schools of the services and does not have specific authority to do so. If NSA is accorded the opportunity to inspect such schools and make recommendations, it is possible that improvements leading toward elimination of unnecessary phases of training and concentration on more important subjects could be effected. (Pages 36-39)

1st Indorsement

To: The Chairman, Commission on Organization of the Executive
Branch of the Government, Washington 25, D. C. May , 1955.

The task force has reviewed with interest Part 1 of APPENDIX I
and concurs with the recommendations contained therein. The importance
of the adoption of Recommendation No. 2 is especially emphasized;
this is believed to be vital to the intelligence effort.

Mark W. Clark, Chairman
Task Force on Intelligence Activities

IX GLOSSARY OF TERMS AND ABBREVIATIONS

AFSA - Armed Forces Security Agency
AFSS - Air Force Security Service
ANEEG - Army-Navy Electronics Evaluation Group
ASA - Army Security Agency
ATTC - Air Technical Intelligence Center

COMINT - Communications Intelligence
COMSEC - Communications Security

DirNSA - Director, National Security Agency

ELINT - Electronics Intelligence

NSA - National Security Agency
NSC - National Security Council
NSG - Navy Security Group

OSO - Office of Special Operations, Department of Defense

SSO - Special Security Officer

USCIB - United States Communications Intelligence Board
USCIBEC - United States Communications Intelligence Board
Executive Committee
USCSB - United States Communications Security Board
USCSBEC - United States Communications Security Board
Executive Committee

T O P S E C R E T

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

THIS DOCUMENT CONTAINS INFORMATION RELATED
TO COMMUNICATIONS INTELLIGENCE AND MUST BE
HANDLED AND STORED SEPARATELY FROM OTHER
TOP SECRET MATERIAL, WITH ACCESS LIMITED
TO THOSE PERSONS DESIGNATED BY NAME ONLY.

THIS DOCUMENT CONTAINS CODE WORD MATERIAL

T O P S E C R E T

ILLEGIB

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

T O P S E C R E T

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

THIS DOCUMENT CONTAINS INFORMATION RELATED
TO COMMUNICATIONS INTELLIGENCE AND MUST BE
HANDLED AND STORED SEPARATELY FROM OTHER
TOP SECRET MATERIAL, WITH ACCESS LIMITED
TO THOSE PERSONS DESIGNATED BY NAME ONLY.

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

T O P S E C R E T

TOP SECRET

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

Report on
INTELLIGENCE ACTIVITIES
in the
FEDERAL GOVERNMENT

Prepared for the
COMMISSION ON ORGANIZATION OF THE
EXECUTIVE BRANCH OF THE GOVERNMENT
by the
TASK FORCE ON INTELLIGENCE ACTIVITIES

APPENDIX I

Part 2

COMMUNICATIONS AND ELECTRONICS IN
SUPPORT OF INTELLIGENCE ACTIVITIES

MAY 1955

THIS DOCUMENT CONTAINS CODE-WORD MATERIAL

TOP SECRET

TOP SECRET

APPENDIX I

Part 2

COMMUNICATIONS AND ELECTRONICS IN
SUPPORT OF INTELLIGENCE ACTIVITIES

TABLE OF CONTENTS

	<u>Page</u>
I INTRODUCTION	1
II SCOPE OF THE SURVEY	2
III TYPES OF COMMUNICATIONS AND ELECTRONICS SUPPORT	3
IV REQUIREMENTS	5
V ADEQUACY AND RELIABILITY OF POINT-TO-POINT COMMUNICATIONS FACILITIES	10
VI COMMUNICATIONS INTELLIGENCE (COMINT)	14
VII ELECTRONICS INTELLIGENCE (ELINT)	15
VIII COMMUNICATIONS SECURITY (COMSEC)	16
IX RELATIONSHIP OF COMMUNICATIONS, COMMUNICATIONS INTELLIGENCE, AND ELECTRONICS INTELLIGENCE	20
X RESEARCH AND DEVELOPMENT PROGRAM	23
XI DUPLICATIONS	24
XII DISASTER PLANS	28
XIII CONCLUSIONS	31
XIV RECOMMENDATIONS	37
XV ANNEX I	42
XVI GLOSSARY OF TERMS AND ABBREVIATIONS	44

TOP SECRET

COMMUNICATIONS AND ELECTRONICS IN
SUPPORT OF INTELLIGENCE ACTIVITIES

I INTRODUCTION

During the survey of intelligence activities, it soon developed that the effectiveness of the whole national intelligence operation was dependent to a high degree on adequate and dependable communications and electronics support. The importance of this can be appreciated better when it is realized that (a) there are more than [] military and [] civilians - for a total of approximately [] - directly or indirectly involved in the overall communications and electronics effort in support of intelligence, (b) this communications and electronics support is costing approximately [] (c) the total value of installations and military equipment especially assigned or available to facilitate utilization of communications and electronics in support of intelligence is in the order of \$300 million, and (d) realistic forecasting, based upon past experience, makes it clear that in the next national emergency the total demands of all activities - both military and civil - for communications-electronics services will far exceed available resources. Obviously, it is important that we know now if these communications and electronics efforts are properly planned, coordinated, and effectively utilized to meet not only peacetime needs, but also those anticipated under the stress of a national emergency. Accordingly, it was determined to make a special survey of the communications-electronics phases of the intelligence activities problem.

25X3

25X3

25X3

II SCOPE OF THE SURVEY

Because of the complexity of the communications and electronics situation in terms of basic similarities and relationships in the technical operations versus wide differences in the objectives and security aspects of the operations, it was deemed in the interest of simplicity to examine the problem in two general directions:

First: To develop information as to what major types of communications-electronics effort are essential to support the overall intelligence operations.

Second: To develop information with respect to controlling factors related to these various types, directly affecting their operational efficiency. Some of the more important are: (a) requirements for normal type point-to-point communications and how they are generated, planned, processed, and provided; (b) requirements for special or unusual electronic operations intended to assist intelligence by interception of radiated signals, either in the regular communications field or in the non-communications field; (c) adequacy and dependability of the facilities available and planned for peacetime and wartime operations; (d) coordination in the planning and operation of the facilities; (e) any unnecessary duplications; (f) disaster plans for key installations; (g) adequacy of national communications security plans and operations; and (h) research and development programs operating to improve the utilization of communications and electronics in support of the intelligence activities.

The survey was made by one staff member added to the task force late in January 1955. The information is based primarily upon visits

TOP SECRET

to and discussion with representatives of the Telecommunication Planning Committee of the Office of Defense Mobilization, the Joint Communications-Electronics Committee (JCEC) of the Joint Chiefs of Staff, Army, Navy, Air Force, National Security Agency (NSA), Army Security Agency (ASA), Army-Navy Electronics Evaluation Group (ANEEG), Air Force Security Service (AFSS), Central Intelligence Agency (CIA), and the State Department. While the quick survey produced broad information on some apparent weaknesses in the plans and operations, time did not permit sufficient followup of discussion and visits to clarify properly many of the points developed, nor to compare actual operations in the field with the descriptions of the planned and actual operations obtained from the "home office." Several items need much further examination or at least detailed spot checks in order that the conclusions and recommendations set forth in this report may be confirmed or revised to meet the true situation, as developed by the more detailed examination.

This report is limited to the survey of the technical phases of the communications and electronics problem. No attempt has been made to determine the validity of the basic or pure intelligence objectives or requirements, which then generate the requirements for the communications-electronics facilities.

III TYPES OF COMMUNICATIONS AND ELECTRONICS SUPPORT

The overall intelligence operation, with the necessarily associated security features, consists essentially of five steps. These five steps and the related communications-electronics aspects are shown below:

1. Production or Collection of Information. This involves radio interception, radio direction finding, of all

25X1

TOP SECRET

TOP SECRET

forms of radio signals which may be reduced to literal text, plus direct battlefield surveillance by electronic means to obtain information from signals which do not reduce to literal text.

2. Assembly of Information for Evaluation. Much of the raw material obtained from the electronic means indicated above, as well as certain other source material collected in the field by other means, must be sent back to the various evaluation centers at home and overseas over the normal radio and telegraph point-to-point communication channels. The demand for this type of communications will increase considerably in time of national emergency. It involves worldwide communications.

3. Evaluation or Analysis. The most advanced and highly complex modern electronics equipment is now being employed at the evaluation centers to speed up the attainment of results and to exploit many analytical possibilities which were not possible several years ago.

4. Dissemination. The product of the evaluation, i.e., the intelligence derived from the analysis, must be sent out promptly to the various users in widely separated locations. This also involves worldwide point-to-point communications.

5. Communications Security. Electronically-operated cryptographic equipment used to insure that the information being transmitted from point to point over our various communications facilities is not divulged to unauthorized persons or nations.

Broadly then, from the communications-electronics viewpoint, there are four general types of operations involved. These are:

1. Standard type point-to-point communications. (COMMUNICATIONS).

TOP SECRET

2. Special communications intelligence operations (COMINT), with its field (intercept) phase and the evaluation phase.

3. Electronics intelligence operations (ELINT), also with a field (intercept) phase and an evaluation phase.

4. Communications security operations (COMSEC), affecting all point-to-point communications operations.

It should be noted that all four types are directly related to standard communications in terms of technical operations and procedures, equipments, training of personnel, research and development aspects, and, most of all - to be effective - they require centralized control with effective decentralized operations.

IV REQUIREMENTS

In each agency surveyed, the generation, evaluation or screening, and procurement of services to meet the requirements followed the same pattern. The basic communications and electronics requirements stem from intelligence requirements established by NSC or USCIB. (These are not being set up properly to permit effective utilization by the communications-electronics organization in developing the maximum communications and electronics potential for gathering intelligence. Efforts are now in process in USCIB to improve the setting forth of these basic requirements.) These basic requirements are then developed in detail by the planners of the various intelligence agencies. Usually at this point the communicators or special communications-electronics advisers join the planning effort. The communications and electronics features of the plan are then prepared concurrently with the basic plan.

TOP SECRET

Requests are made, whenever this is considered feasible, on one of the existing government communications services to provide point-to-point communications services. For example, NSA presents its point-to-point communications requirements - both immediate and on a three-year forecast basis - to the JCS who then (through JOEC) allocate responsibility for providing the required service to one or more of the military services. CIA operates on a somewhat similar arrangement, except that CIA deals directly with the different military services, each of whom for security reasons, has designated a special liaison officer to handle CIA requests. In special cases, where the military services do not have available facilities, CIA provides its own, or leases facilities from one of the commercial communications companies. An example of this is where CIA has installed, operates, and maintains a special long-line overseas radio circuit to the South and leases submarine cable facilities to Europe. State Department also leases commercial channels to Europe to reinforce facilities furnished to State by the military networks.

The demands for point-to-point communications services of the Army, Navy, and Air Force intelligence activities are realistically screened by the chiefs of the respective communications services, to determine validity, technical soundness, and how best to meet the demands. The CIA Director of Communications screens the demands for CIA and then presents them directly to the Army, Navy, or Air Force for supply of service. The Army, Navy, and Air Force do not challenge the requests from NSA or the civil intelligence agencies unless they are unable to meet them, in which case they will try to adjust the demand against what is available, or arrange through the Secretary of Defense or the requesting agency for additions to be made to their military facilities to meet

the requirements. NSA establishes its own demands and then presents them to JCS, who do not challenge or examine the justification for the requirement, but try to furnish by allocation of responsibility for furnishing the service to the Army, Navy, and Air Force. If the JCS are unable to furnish, they try to adjust by negotiation or will plan with the military services and the Secretary of Defense for additions to the military networks to meet the NSA demands. Generally, this method of handling the requirements and the resultant arrangement for provision of point-to-point communications services represent a so-ordinated, sensible way to deal with the problem, except for one aspect. There is room for improvement with respect to insurance of economy and realism in the development of CIA and NSA point-to-point communications requirements - at least in principle - if these requirements are to have the benefit of objective evaluation by an authority other than the actual operating authority. Technically qualified authority, not involved in the actual operation, should review and comment to the department heads or directors concerned on any major or special type communications or electronics proposals of intelligence agencies to insure that they are basically sound and realistic. Whenever possible, these facilities should be provided from existing services or facilities. This would provide a suitable check on any future tendencies to go "luxurious" or to get unrealistic in the face of anticipated conditions likely to exist in the general communications-electronics effort in wartime. It would appear that the Joint Chiefs of Staff with its existing JCEC group of highly experienced and technically qualified personnel could effectively provide this particular advisory service

TOP SECRET

for such agencies in a manner that would be in the best interests of the Government. This could be done by direction of the Secretary of Defense for NSA. It could be done through the Secretary of Defense, at the request of any intelligence group at USCIB level, for activities not a part of the Department of Defense.

The requirements problem related to the developing, processing, reviewing, and implementation of communications and electronics plans in support of communications intelligence and communications security areas appears defective in two major aspects: (a) there appears to be no provision for an objective technical review of the basic communications and electronics requirements plan generated from the admittedly unsatisfactory USCIB statement of basic or pure intelligence requirements, and (b) there appears to be no effective provision for an objective technical review of the communications and electronics equipments, facilities, and personnel requirements developed from (a). It should be noted that whereas most of the point-to-point communications requirements have the benefit of some technical guidance from the military communications services - although this is purely aimed at utilizing to the maximum existing facilities and does not touch the basic or initial justification of the need for the service - in the area of special communications intelligence and communications security, the intelligence activities set up their own requirements in terms of personnel, equipment, and funds. (This is primarily an NSA area, with NSA being directly supported by ASA in the Army, NSG in the Navy, and AFSS in the Air Force.) For example: development of requirements in the COMINT effort for intercept positions. This involves such factors as (a) operated by all foreign governments

[redacted]

on a worldwide basis, (b) number of

military [redacted]

(c) which links should be fully guarded

in peacetime, (d) how many additional links anticipated in wartime,

(e) what changes and additions in coverage to be made in wartime, (f)

when, where, and by whom the selected links can best be covered, (g)

duration of coverage. Every one of those questions involves fundamental

communications and radio problems. Every one is related to the total

wartime communications and electronics capability in the light of esti-

mated available resources. Should the number of intercept positions

in peacetime be

[redacted]

[redacted]

25X3

25X3

Every position involves highly trained personnel, complex and expensive equipment, effective engineering guidance in location and installations. It clearly is proper that those with COMINT responsibility should develop the basic plan to include setting up the requirements in terms of personnel and equipment to meet the requirements. It is of the greatest importance that such a plan - such sizeable requirements - receive the benefit of review by the best qualified group available with suitable operational experience in the communications fields to (a) determine the overall realism of the plan, (b) determine its soundness from the technical viewpoint, (c) see if it makes full usage of available means, (d) determine the impact of the plan on the overall communications and electronics requirements for all Federal operations in time of emergency. It is stressed that these communications intelligence and communications security field operations are today, and in the future will be, mainly military operations. They cannot be measured mainly on civilian

25X

25X1

25X3

TOP SECRET

"norms," which do not necessarily apply to military operations. They should not be measured in overenthusiasm of intelligence personnel who obviously do not appreciate some of the long-range implications or significance of this communications and electronics "means." It is not definitely concluded from this brief survey that inappropriate, or unnecessary, or uneconomical demands are being made and implemented in this area, but there are certain clear signs that (a) there already are some unnecessary duplications of effort occurring, and (b) some of the thinking and operational objectives verge on wishful thinking, tend to ignore realities, and may require radical changes in times of emergency. The definite conclusion is that some effective plan should be set up so that those at high levels and required to make policy decisions would seek out and have available to them the advice and guidance of those who have a wealth of know-how, those who can give them an unbiased, objective evaluation of proposals, those who will most likely in the final analysis make the overall communications and electronics military plan work. The chiefs of the military communications services, the Director of JCEC of the JCS, and their staffs contain a wealth of know-how, based upon experience. It is not clear that such advice and guidance have been sought out or effectively used by those at high level dealing with this highly technical and expensive facet of intelligence operations.

V ADEQUACY AND RELIABILITY OF POINT-TO-POINT COMMUNICATIONS FACILITIES

For peacetime, there exists a comprehensive, integrated network of communications both in the United States and to all important overseas areas, especially where military forces are stationed, that is considered

TOP SECRET

both adequate and reliable to meet the requirements of the whole U.S. intelligence community.

For wartime, there may be more facilities actually available than at present, but the reliability factor will become a matter of major

concern. [REDACTED]

25X1

[REDACTED] to cause

considerable disruption of both the strategic long-line radio circuits and the short-haul tactical circuits. Additionally, there will be the (a) heavy traffic loads normal to wartime operations, (b) normal atmospheric interruptions, and (c) periods when combat operational priority demands will require readjustment and allocation of all available long-line circuits. In such a situation, the extensive and well-integrated radio communication networks of the three services, plus the cable facilities, will be able to move traffic over arterial long-haul circuits, but this will involve much rerouting of traffic, rearrangement of circuits, and heavy utilization of common-user facilities. The serious implications to intelligence operations are obvious. The antidote is maximum coordination and integration of communications-electronics planning in peacetime.

There is clear warning here to all intelligence agencies not to get too dependent on equipment which may require special full-time channels. This relates directly to some of the present and planned communications security equipment requiring numerous "on-line" full-time channels. For example, in the United States, on overseas links and within overseas theaters, the Air Force now operates more than one hundred "on-line" channels. NSA has some fifty-six in the Washington area alone. Most of these are operating over land-lines and some are operated in the overseas

25X1

channels. However, many "on-line" channels within the overseas theaters involve land-line circuits obtained from local civil communications companies. The availability of these facilities in an emergency cannot be guaranteed, since they are not under U. S. control and will be subject to both sabotage and possible enemy action. Generally, the chances are many of these channels will be lost to the intelligence activities. This means there may be wholesale shuffling of communications arrangements, with heavy dependence on common-user systems, just when the facilities are most needed. All of this emphasizes the need of effectively marrying day-to-day training and operations to the realities of a wartime situation; i.e., be sure the intelligence activities can operate effectively on what is available. It is not too clear that such realism governs operations in some of the intelligence agencies.

One of the major factors in bringing about dependability in over-all communications is the capability of rerouting traffic in emergencies or because of man-made or natural interference. This capability of "getting the message through" is dependent to a high degree on effective integration of various communications networks and the necessary standardized operational procedures so that the setting up of special circuits or the passing of traffic over any available facility can be done in a routine fashion. This situation exists to a high degree in the worldwide networks of the Army, Navy, and Air Force. They are improving their capabilities in this direction every day by improved operational practices, with tested new equipments and additions to the systems' capacities and routings.

The major long-line communications networks within the United States

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
have a very high degree of dependability from the technical viewpoint.

However, these facilities could be seriously affected by strike action, deliberate sabotage, or by ineffective operation of priorities and controls of personnel to restore essential national communications services promptly to key intelligence activities in wartime or in case of disaster.

At this time, the intelligence activities obtain their requirements from the existing and well-integrated military and civil networks for overseas communications. They have access to the world's best communications facilities within the U. S. borders. The intelligence activities are reinforcing their overseas facilities obtained from the military by leasing circuits from commercial communications companies whenever the military are unable to meet the demands. This arrangement is basically sound, economical, and certainly in the best interest of the Government. In this area, there are times when the "eager beavers" or the "empire builders" demand expensive type circuits for their own special purposes. Any such tendencies should be resisted firmly. That is why there is need for an effective and realistic screening of all requirements for communications services to uncover promptly any demands for what may be called "luxury services."

The present arrangements provide the maximum in obtaining adequate and dependable communications services and facilities for the national intelligence agencies at the minimum cost to the Government. They provide reasonable assurances that the adequacy and dependability can be maintained in time of national emergency. These arrangements should be continued. Any attempt to set up separate communications systems or facilities, which duplicate existing facilities

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
should be vigorously resisted.

VI COMMUNICATIONS INTELLIGENCE (COMINT)

The Director, NSA, operating directly under the Secretary of Defense, is responsible for the effective planning for and utilization of available communications intelligence collection and processing resources of the United States to meet U. S. intelligence requirements. (NSCID No. 9 establishes USCIB and designates the Secretary of Defense as the executive agent. The Secretary of Defense has delegated this full responsibility to NSA.)

Communications and electronics operations are the major means available to carry out this mission. The requirements generated by USCIB Statement of Requirements and restated by NSA planners are complex, covering several facets of communications. They are large in quantities when measured in communications services, equipments, and personnel to operate the equipment. Essentially, they require rapidity of point-to-point communications, ability to transmit all messages over such systems encrypted, and necessary exclusive-use channels to permit such transmissions.

The present plan, whereby the Army, Navy, and Air Force provide the majority of the communications services and the units to operate in the field the NSA intercept and direction-finding (DF) missions, is an effective and realistic way to meet the problem. The whole NSA field operation, related closely as it is to communications, has certain inherent characteristics of communications. For example: (a) the principle of centralized control necessary to any efficient sizeable communications network is obviously needed in the NSA operation; NSA has this. (b) De-

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

centralized operations with due regard to local area situations and ability to operate with maximum efficiency in time of major emergency; NSA has this only in part. Since its overseas customers are essentially military, it has certain principles of command also involved. The Director, NSA, is aware of this and is moving toward better decentralization. Such decentralization will be helpful in times of national disaster or in case of war.

It was noted that a new school for special type equipment for intercept of radio teletype signals was being set up in California by the Air Force. The Navy expects to participate.

From the national interest viewpoint and in the interest of economy in use of resources, every effort should be made to insure that NSA utilizes to the maximum all available facilities, services, and equipments rather than become involved in setting up any duplicate or parallel arrangements.

VII ELECTRONICS INTELLIGENCE (ELINT)

ELINT - that part of the intelligence effort which deals with the interception of electronic emissions or signals not carrying regular communications - is a comparatively new member of the intelligence team. It has evolved over the past few years from the pioneering of the military services who have a high interest in radiating signals which may be related to electronic devices or equipments used for guiding missiles, or for energizing electronic equipments which are being used as weapons. Such information is most helpful in locating and unmasking enemy offensive operations. These things are real, vital, and of immediate concern to the military services. The Army and Navy have a

TOP SECRET

joint arrangement wherein the raw material intercepts are analyzed at a central point. Any product of this analysis is distributed to the three services and to NSA. The Air Force is operating independently, but does maintain liaison - not believed to be very effective - with the Army and Navy. Their analysis is being done, first, in overseas theaters, and, secondly,

25X3

25X3

There is need for an organization with a central authority to bring about a much better coordination in the overall planning, overall operations and analysis of the raw materials, and then to insure that there is full dissemination and proper utilization of the product. The absence of such an arrangement contributes to duplication of effort in some areas while important gaps could be present in others. Any plan which would result in the setting up of a central authority for ELINT should include full consideration of the very immediate and direct interest of the military services in this particular field. Such plan should insure control of electronic countermeasures (ECM), a tactical weapon to the military commanders concerned.

A plan to correct this situation, generally agreed to within the military services, has been under discussion at JCS, Defense, and CIA level for several months. There is need for decision and implementing action.

VIII COMMUNICATIONS SECURITY (COMSEC)

Communications security, as discussed herein, relates to measures taken to protect from unauthorized persons classified information

TOP SECRET

transmitted via electrical means from point-to-point. It pertains to cryptographic systems, cryptographic equipment, and cryptographic operational procedures.

Responsibility for effective communications security in the United States has been placed by NSC on USCSB. USCSB, in turn, has delegated the responsibility to the Secretary of Defense as the executive agent to take all necessary actions. The Secretary of Defense has designated NSA as the agency responsible for supplying necessary materials (equipment and systems) and for necessary technical guidance with respect to utilization of the materials by the various departments and agencies. The departments and agencies are responsible for communications security operations. This is considered a feasible and an effective arrangement.

NSA does in fact develop, manufacture, and distribute, on a wholesale basis, cryptographic systems, as required, to all government agencies. NSA develops and procures all needed manual or electronically operated cryptographic equipment and, as necessary, manufactures within NSA certain essential parts of these equipments. They are then issued with necessary operating instructions on a wholesale basis to government agencies. Additionally, specified security violations involving possible compromise of cryptographic systems are reported to NSA where it is determined by careful evaluation if an actual compromise of a system has occurred, how serious it may be, and what corrective action should be taken. Departments and agencies concerned are promptly notified of corrective action needed. Corrective actions are then taken by the departments concerned. (Security is a command function in the military services.)

CIA and State Department use systems and equipments provided by NSA. They also produce certain special codes for their own use. There exists liaison with NSA on these to insure adequacy of security being developed.

There exist codes which permit worldwide exchange of information on a secure basis between the various U. S. departments and intelligence agencies.

NSA, CIA, and State Department all indicate stockpiles of some reserve equipment and sufficient systems, at locations well out of target areas, for emergency use. NSA felt its equipment reserves might not be adequate for a major national emergency of any real duration since it is unable to procure these equipments - which require months of lead time - except to meet specific requirements.

Reports of possible cryptographic compromises, directly related to communications intelligence operations, during the period March 1, 1954, to February 28, 1955, showed a total of 1,330 (including 850 possible cryptographic) errors in transmission, 260 messages lost or misplaced, and 220 possible communications intelligence compromises. Further careful evaluation of the situation indicated the probability that only two of these compromises were considered to endanger current or future operations, and these two for less than four days. This would indicate a generally good situation in this particular area. The majority of these security violations are due to human errors; this, in turn, is due to the great turnover of personnel, especially in the military services.

It should be noted that the above figures are limited to possible compromises of communications intelligence (NSA) traffic, which is

TOP SECRET

considered the most sensitive and provides a high percentage of the total encrypted traffic carried over the worldwide military networks. To get a true overall picture of the general communications (cryptographic) security situation, figures affecting the handling of coded traffic by the major networks in all areas and for other customers or activities must be considered. Specific figures were not available from all agencies, but broad figures obtained from JCEC of the Joint Chiefs of Staff indicate the general situation for a period of approximately one year, insofar as the Army, Navy, and Air Force operations are concerned, to be substantially as follows:

- | | |
|--|-------------|
| 1. Number of messages sent | 790,000* |
| 2. Number of chances for security violation in handling messages in 1. | 3,950,000** |
| 3. Security violations considered of sufficiently serious nature actually to endanger cryptographic security | 8 |

From the above, it appears that (a) the overall communications (cryptographic) security situation is very good and (b) with full

* This figure does not include (a) multiple address type messages requiring utilization of more than one crypto system and (b) additional messages developing from breakdown of long messages into several for ease in transmission. These additions would add approximately ten percent to the above for a total of about 870,000 messages.

** Complete transmission includes five handlings or chances for crypto security violation: (1) encryption, (2) sending, (3) receiving, (4) decryption, (5) handling at relay stations.

TOP SECRET

TOP SECRET

recognition of the fact that even a single violation may result in a compromise of a crypto system or in giving valuable information to a potential enemy, nevertheless realism in terms of number of serious security violations (8) measured against number of chances for violations (3,950,000) makes it appear that no major change or corrective action is needed at this time. The continued vigorous implementation of the present programs should adequately meet the situation.

It is stressed that all of the above deals with communications security in terms of cryptographic systems, cryptographic equipment, and cryptographic operational procedures. It does not pertain to the much broader field of messages sent in clear text over military networks or over civil networks by order of the sender. These often include valuable information of assistance to the enemy. This situation, in contrast to the cryptographic area, appears quite weak. This problem is not under the communicators control. The operation extends beyond the military service. It needs attention at NSC level.

IX RELATIONSHIP OF COMMUNICATIONS, COMMUNICATIONS INTELLIGENCE, AND ELECTRONICS INTELLIGENCE

One of the most effective, if not the most effective, means of getting information is via electronic means. In its simplest, most used, and basic form, this is interception of electro-magnetic or radio signals regardless of whether they are being used to carry information (i.e., messages) or to control equipment or weapons (i.e., radar,

etc.).

If this is so, then maximum know-how and experience available in the radio area should be brought in support of the whole COMINT-ELINT effort. Those with years of experience and a wealth of know-how directly

25X1

25X1

TOP SECRET

related to this type operation are the communicators, especially those in the military services.

It is of high importance that the effort not be handicapped by organizational concepts which tend to separate the COMINT and ELINT operations from communicators who can help in attaining maximum results in operations, training, research and development, and especially in providing technically qualified personnel to assist in operations. Such help will be of greatest importance in time of emergency.

On the other hand, since the operational objectives of those communicators operating in the intelligence field is quite different from the standard communication objectives, it is apparent that there may well be a need for a special service directed to the special objective. But any such plan should keep clearly in mind the technical fundamentals involved. To insure that maximum effectiveness in terms of economy in utilization of personnel, equipment, and facilities, as well as the available potential, is achieved, all organizational and operational concepts should include full participation and coordination of the maximum know-how available. Any attempt to separate or duplicate in these areas should be vigorously resisted.

The tendency to place non-communications personnel in key command and staff positions, where the operation is concerned mainly with communications and electronics, is detrimental to the effort in terms of lost momentum while new personnel are receiving the veneer coating of instruction to fit them for assignments involving many technical considerations, and the understandable unwillingness of many of the best and most experienced technical communications type personnel to work on such a team at lower operating positions and without much hope of

attaining the higher positions. Authorities, commanders, and staff officers at posts involving decisions and policy making on communications and electronics matters should be assured that they base such policies and decisions on sound, realistic know-how, usually available to them on call from those in their respective services or operations. They should assure themselves of the technical competence of those advising them or the sources of the advice on matters heavily weighed with communications and electronics implications. It is stressed that these comments apply to the communications and electronics technical facets. They do not relate to the need in those organizations for analysts, intelligence personnel, etc.

It appears that there is a real need for much better appreciation at top levels in the whole intelligence community - both civil and military - for the dependence of intelligence activities for success on adequate and dependable communications and electronics support, to appreciate better the magnitude of a communications-electronics operations in support of intelligence, and the potential of communications-electronics to meet some of the collection problems which appear to be almost insoluble by other means.

This development of a better appreciation might be accomplished by a carefully integrated, effective program of instruction to be given to selected key personnel at top levels in all departments who are involved in intelligence operations, and incorporated in the courses at the several governmental colleges such as the National War College, Industrial College, State Department schools, etc. The course should be broad enough so that it could be given to anyone with a

Secret or higher security clearance.

Another step in the direction of improving this situation would be to utilize much more effectively the wealth of know-how and experience available in the JCEC of the Joint Chiefs of Staff as advisers on all communications and electronics facets related to intelligence proposals. For example, the Secretary of Defense, all ^{service} Secretaries, and especially civilian staff members at the Secretaries' level, confronted with problems pertaining to military communications or electronics, should insure that the JCEC comments - military and technical - are available to them to assist in arriving at proper decisions. The JCEC is particularly well qualified to suggest steps to be taken to resolve conflicts as to ^{particular} operations with respect to placement of responsibilities on the various agencies for provision of communications-electronics facilities and for further exploitation of possible new methods to use communications and electronics to improve our overall intelligence operations.

X RESEARCH AND DEVELOPMENT PROGRAM

The research and development program in support of special communications intelligence operations and communications security activities is conducted under direction of NSA. It is considered to be well organized, ably directed, and generally very effective in insuring the superiority of United States equipment over similar equipment of other nations. To insure that its program is abreast of the latest scientific developments in the world, NSA has organized the National Security Agency Scientific Advisory Board which has on its membership outstanding leaders in the scientific world in those areas in which activities of the agency fall. In addition to the talent on

this board, NSA has a staff of top level consultants and experts in a variety of fields who participate in the research, development, and production programs to lend their knowledge and experience. Projects and studies in progress include, for example, speech security programs, mathematical techniques related to crypto principles, electronic techniques for incorporation of new principles into compact, secure, reliable equipment, special equipment and techniques for intercept operations, and many others.

Although the benefits and assistance of research and development efforts of the Army, Navy, and Air Force, and civil communications-electronics developments are brought to the support of the effort, there are indications that overemphasis on security by NSA personnel restricts the real potential available for this source, and may permit expensive, time-wasting duplication of effort. (See page 27)

The research and development effort in support of the electronics intelligence operations has very capable potential support available from the research and development efforts of each of the three services and, undoubtedly, can be helped by the NSA research and development effort. However, there is need for better coordination in evaluating the whole problem and in coordinating and allocating responsibilities to permit more effective progress of this effort.

XI DUPLICATIONS

The survey disclosed four general areas of actual or probable duplication:

1. Operations. In the operations within the larger relay and communications centers, both in the United States and overseas. Under

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0
the present plans, it seems that there may be unnecessary duplication of cryptographic operational personnel and duplication of equipment and maintenance men. There is a growing tendency for intelligence activities and agencies - primarily NSA - to become involved in this type of strictly communications service on the basis of need for increased speed of delivery of traffic and because of special security features pertaining to their traffic. NSA is now planning to use Centralized COMINT Communications Center (CCCG) relay operations. Automatic switching equipment - an important element of this system - is just being tested on land-line circuits within the USA. It has not yet been tested on radio links. Such relay centers, as separate entities, are not likely to be available for at least eighteen months. It may be three to five years before network operations will be practical. These are basic point-to-point communications matters which should be handled by those responsible for communications. (It is understood that NSA actually would prefer the military communications services to operate part of such a system, at least initially.) If NSA gets into this field, not only unnecessary duplication of effort will result, but if the main NSA relay centers are physically separated from the larger major relay centers, they simply are inviting trouble in times of emergency when they will have to fall back on the major military networks for help. When this happens, it will be much better to have the maximum of point-to-point communications control under direct supervision of those responsible for operating the basic communications systems. The enthusiastic desires of NSA and others for reduction in delivery time of messages is commendable and should be a target for all to attain. The military at all command and staff levels should insure

25

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

TOP SECRET

proper support to their respective communications services so that they may provide such service for NSA, and all other customers, as soon as practicable. Such action would decrease the growing tendency toward duplication. Actually, it should produce much more dependable service to the intelligence agencies in wartime.

2. Training. There are evidences of possible duplications in the training efforts within the separate military services, especially as it pertains to the basic training of personnel to be used in special electronics or communications security fields. (This observation applies to training within individual services. It is agreed in principle that communications and electronics training should be done by each service because of variations in many of the operational aspects; i.e., Army - land stations, Navy - at sea, Air Force - in planes.) For example, the Army since before World War I, has operated excellent schools for training Morse code and CW (continuous wave) operators, or other special type radiomen, and fullscale officers communications courses. Recently, the ASA (Army part of NSA) began operating at another location, and is gradually expanding what appears to be generally duplicate courses. In officers courses totaling approximately 1,400 hours, more than 1,000 hours are subjects which it appears could easily be taught - and equally well - at the established Signal Officers School. A few special instructors or a team from ASA could then come in and provide instruction for the balance of 400 hours. A similar situation exists with respect to courses for training radio intercept operators. While additional space is needed at the new location, ample space, facilities, and know-how seem to be available to cover these courses at the existing Signal

TOP SECRET

schools. (It was noted that the Air Force appears to be using effectively available facilities for basic specialist training of their radio intercept operators at Keesler Air Force Base.) It appears that one difficulty here may be a formula and method of setting up these training efforts, where staff officers - not technically qualified - are making decisions based on a so-called MOS (Military Occupational Specialty) without realizing the technical implications involved in the specialties.

3. Research and Development. There is a very real possibility that duplication is occurring in this area due mainly to overemphasizing the security factors on a piece of equipment as such and on the statement of technical requirements in terms of technical characteristics and technical objectives. In such a situation, considerable duplication of effort could occur simply because those who already had done work in the particular area, or who may even have the complete answer, did not know the problem was a matter of active interest to NSA. There should be a distinction between the piece of equipment as such and the specific operational objective for which the equipment is needed. This situation does not appear to be from top level policy, but stems from overconscientiousness at the working level, where the motto sometimes appears to be, if in doubt, settle on top special security.

4. Requirements. The absence of an effective and objective unbiased review of the basic communications and electronics requirements - to include justification therefor - by a well-informed, technically and operationally experienced group not involved in the actual intelligence operation, obviously opens the door to unnecessary duplications and

and extravagant or inefficient utilization of the always critically short communications and electronics resources. Such situations could easily develop from enthusiastic, well-intentioned efforts to attain objectives, but where available information and objective viewpoint have not been fully utilized. Overemphasis of security or demands for priority of requirements should not be allowed to foster such a defect in basic controls. This brief survey did not permit a proper exploration of this matter.

This whole area needs detailed and objective study by qualified and experienced technical personnel to insure that there are no unnecessary duplications of effort in our peacetime operations and that operations are geared realistically to the wartime situation. Any rearrangement of existing operational activities and responsibilities would have to be done very carefully to avoid interruption of essential traffic, especially with respect to operations and training.

XII DISASTER PLANS

The key communications-electronics facilities to support the major part of the intelligence collection and evaluation effort are located directly in one of the highly publicized and obvious nuclear weapon target areas; i.e., Washington, D.C. These facilities are the focal points for the reception of specially coded COMINT type traffic from all parts of the world. They contain the heart of the day-to-day operations from which the communications-electronics information is obtained to keep current the national intelligence estimates of the world situation. In time of national emergency, they become of the highest importance.

Realistic planning applied to these facilities should be the same as applied to any other key military installation on which considerable dependence is placed when a national emergency occurs. This should provide as the absolute minimum that in case of disaster or heavy sabotage there are alternate locations definitely agreed on; that the necessary minimum installations of equipment and connecting communication facilities have been made and tested in these locations; that key communications, electronics, and analytical personnel are definitely instructed as to what they are to do in case of a need to move to these new locations. Additionally, the satellite or related intelligence communications installations should have a clear understanding of the broad disaster plan, and particularly what actions or responsibilities may fall to them in such an emergency. Further, it should be a fundamental policy that the planning of any additional critical intelligence installations directly into known target areas, would be avoided.

The preliminary examination of this problem indicated that in case of disaster:

1. NSA had originally planned to move its operations to the University of Maryland area. This particular plan has been overtaken by recent developments with respect to target areas and is no longer considered satisfactory. A new plan has been adopted to move the major communications intelligence activities of NSA from the city of Washington to Ft. Meade, Maryland. Implementation of this plan has started. However, it will not be completed for nearly two years. It should be expedited. NSA has initiated planning of an alternate location for the Ft. Meade installation, but advises that they have been unable to date to get agreement with responsible government planning agencies as to

where their new alternate location - after they move their main effort to Ft. Meade - could be situated.

It was further indicated by NSA that some of the expensive and hard-to-replace fixed plant type of electronics equipment would be ready for use in a possible alternate location in the Midwest within a matter of two or three months. Additional standard type IBM equipment, to be procured later, would also be utilized in the new setup.

The present plan of the Director, NSA, to decentralize certain of his evaluation effort directly to the overseas theaters might compensate to some degree for the loss of production facilities in the Washington area. Implementation of this decentralization is just starting. It should be expedited and it will need to be on a basis of realism as to what may happen in the particular overseas area.

The interim thinking of NSA seems to be that if their main facilities were lost, then the AFSS facility in San Antonio could carry some of the immediately essential part of their load until NSA could resume operations elsewhere.

It appears that the AFSS facility at San Antonio might be able to carry approximately ten to twenty percent of the NSA load, provided that they were given some additional equipment and were reinforced by qualified analytical personnel. However, the AFSS commander states that he does not know of this plan. (This raises the question as to how well coordinated and integrated these disaster plans are at this time.) He further pointed out that the AFSS alternate arrangement calls for transferring their operations in case of disaster to one of their smaller operating units on the West Coast. The West Coast installations

TOP SECRET

would be able to handle only a small part of the present AFSS load; in fact, it is intended mainly as an alternate headquarters for AFSS until AFSS could be reorganized.

Although the above situation essentially concerns communications intelligence, communications electronics, and communications security installations, standard type point-to-point communications in these locations are also involved. It is probable that the standard type communications - provided the main line circuits are made available at the alternate locations and rerouting plans are ready in advance - could be put back into operation fairly quickly.

The current disaster planning situation with respect to the key communications intelligence facilities is not good. This applies specifically to the concentration of the major part of the highly specialized electronics evaluation equipments in the heart of the admitted target areas. They could be lost in one quick disaster. Further, there is no alternate establishment satisfactorily set up and ready to carry part of the load immediately, in case of disaster. It would be months before normal operations could be resumed. There is need for prompt, comprehensive, and coordinated planning to insure that all agencies know what to do under the probable disaster conditions. All such plans should insure readiness of some alternate facility to take over. These plans should be known to all key members of each activity and to heads of other activities of the intelligence community.

XIII CONCLUSIONS

Conclusion No. 1

There is a need for a more realistic statement of requirements from

TOP SECRET

TOP SECRET

USCIB (or the Combined Intelligence Board recommended as a replacement) to the intelligence agencies concerned with communications or electronics intelligence capabilities, so that communications and electronics resources available to such agencies may be better directed on suitable targets and to permit better exploitation of the potential of this means of producing intelligence. (Page 5)

Conclusion No. 2

Technically qualified authority - not involved in the action operation - should objectively review and comment to the Combined Intelligence Board* or to the department heads or directors concerned, on any major or special type communications or electronics proposal of intelligence agencies to insure that they are basically sound, realistic, properly coordinated, and have been formulated with due regard to economy and existing facilities. This applies particularly to communications and electronics requirements as developed by CIA and NSA. Because of the direct relationship to national defense and the security aspects of these operations, and since a high percentage of the operation is accomplished by the military, it would appear that the military services (JCRC) might best be qualified and equipped to provide, on request, this review and advisory service.

(Page 7)

Conclusion No. 3

The present basic arrangement whereby the intelligence activities obtain their point-to-point communications services from existing governmental communications services, or by leasing of commercial services rather than operating their own, is sound. (Page 13)

*If USCIB and USCIB are combined as suggested in Part 1 of this Appendix. Otherwise, report to USCIB.

Conclusion No. 4

It is not clear that full utilization of existing facilities, personnel, equipment, and know-how is standard practice with respect to communications intelligence and communications security operations. This situation is related to the tendency to overemphasize some of the security aspects. The policy in these areas, with due consideration of essential security aspects, should fundamentally be the same as for point-to-point communications support; i.e., maximum utilization of existing facilities. (Pages 8-9).

Conclusion No. 5

Point-to-point communications facilities appear quite adequate and reliable to meet peacetime requirements of the intelligence activities. (Page 10)

Conclusion No. 6

It is doubtful that the point-to-point communications facilities will be sufficiently adequate or reliable to meet all the foreseeable wartime requirements. This wartime situation will directly affect the availability of special, full-time channels required to permit utilization of some of the communications security equipment being used extensively in peacetime and planned for extended use in wartime. Effective wartime communication will require extensive recourse to "common-user" facilities. Planning of facilities and day-to-day operational practices should include a full appreciation of these wartime realities. (Page 11)

25X3

Conclusion No. 7

There is good evidence available to indicate that

25X3

This capability probably will increase in effectiveness in time

goes on. As a result, communications and electronics efforts in support of intelligence will be directly and adversely affected. Planning must include realistic consideration of this factor. (Page 11)

Conclusion No. 8

The present basic arrangement, which places full operational control responsibility for communications intelligence on the National Security Agency, is sound. However, it appears that further decentralization of this operational control would improve the overall operational effectiveness, not only technically, but particularly in times of national emergency. (Pages 14-15)

Conclusion No. 9

The present plan covering the organization of the electronics intelligence operation is definitely weak from the technical operating viewpoint. As presently organized, the potential of this means of collecting intelligence is not being exploited properly. There is need for an effective coordinating authority. Planning and discussions on this subject have been in progress at department level for several months. Because of the direct importance of this means of intelligence to the military, agreement should be reached quickly and directives issued to bring about the needed coordination to develop this potential. (Pages 15-16)

Conclusion No. 10

Emergency or disaster plans for the key communications-electronics activities in support of intelligence - especially of the National Security Agency in the U. S. area - are considered generally weak. NSA is in process of moving its main installation to a better location, but the process needs to be expedited. NSA is searching for another alternate

TOP SECRET

location and needs more effective help from Federal authorities charged with allocation of such locations. There is need for more positive, prompt, comprehensive, and coordinated planning in this area, since it affects the whole national intelligence community. (Pages 28-31)

Conclusion No. 11

The U. S. telecommunications security (cryptographic) effort appears to be well organized, well operated, and to afford adequate security. It is centrally controlled as to equipment and systems with decentralization of operations to the various departments and agencies. The total number of communications cryptographic security violations, compared to chances for security violations, is very low. The number of actual compromises, based upon expert evaluation, is extremely low. There are active, continuous, well supervised programs of instruction and inspection in the agencies, with effective reporting procedures aimed at further improving the overall cryptographic security operation.

There is a definitely weak telecommunications security area with respect to the transmission of clear text messages, sometimes containing information of value to the enemy and ordered sent in the clear by the senders. This involves both government and civil agencies. It reflects in telecommunications operations, but is not under the control of telecommunications authorities. This area should be examined by the National Security Council. (Pages 16-20)

Conclusion No. 12

Research and development efforts to produce new communications and electronics equipment and techniques in support of special intelligence and communications security activities are vigorous and considered very

35
TOP SECRET

TOP SECRET

effective. The benefits of research and development by the Army, Navy, Air Force, and industry in the general communications-electronics field are also being integrated in the research and development program. One facet needs attention; see Conclusion No. 13. (Pages 23-24)

Conclusion No. 13

There are sufficient signs to indicate the need for careful, coordinated, and objective study of present and developing duplications of effort in the following areas: (a) operation of separate tape relay centers in intelligence activities when such service exists and can or could be provided with some modification by the regular military communications services; (b) establishment of certain additional courses and separate training facilities for communications and electronics type operational personnel within the respective military services, when the facilities, and especially the know-how, for the major part of such courses could be provided from existing facilities within those services; (c) tendency to overemphasize security in dealing with research and development equipment and techniques of a communications or electronics nature and intended for special type intelligence operations. Unnecessary duplication in these areas in peacetime can lead to unnecessarily high cost in wartime, not only financially, but also in wastage of critically needed technical manpower and highly technical equipment. It is stressed that this problem should be examined by personnel combining considerable operational experience and technical know-how in the communications and electronics fields. The only existing agency found which might provide an effective, unbiased service in this field was the Joint Communications-Electronics Committee of the Joint Chiefs of Staff. (Pages 24-28)

36

TOP SECRET

Conclusion No. 14

There have been unseemly long delays in reaching agreements on some of the proposals submitted to higher authority from responsible operation levels and which are needed to make the electronics effort in support of the intelligence activities more effective. (Example: the proposal for organization of the electronics intelligence operation.) This appears to stem from difficulties in getting agreement within the military services on certain aspects of various problems, lack of sufficient authority in the Joint Chiefs of Staff to make command decisions in these matters where agreement is difficult, and the obvious lack of adequate and suitable types of field and operational experience by some of the military and civilian authorities who are trying to deal with these highly technical and specialized problems containing important military command and operational aspects. High level civilian authorities have access to very competent and responsible personnel in their organizations, with long experience in these areas, but it is not clear that such counsel is required, sought, or properly used. (Pages 16, 23)

XIV RECOMMENDATIONS

Recommendation No. 1

That an Intelligence Communications and Electronics Subcommittee (ICES) to the Combined Intelligence Board* be established to review and produce recommendations to the Combined Intelligence Board with respect

* This assumes that USCIB and USCSB have been combined into a single board, as proposed elsewhere in this report.

~~TOP SECRET~~

to all communications and electronics proposals from intelligence activities which call for facilities, equipments, or additional personnel which cannot be obtained from existing resources; and to supply technical advice to the Combined Intelligence Board on such matters as they may request. Proposed composition and terms of reference are shown in Annex I attached hereto.

Recommendation No. 2

That more effective use be made within the Department of Defense of the high potential value and know-how available in the Joint Communications-Electronics Committee of the Joint Chiefs of Staff to deal with communications and electronics problems related to the broad intelligence field. Responsibility should be placed on that group for reviewing and commenting on communications and electronics requirements that the National Security Agency considers necessary to meet the intelligence objectives, and the demands being placed by NSA on the special communications and electronics groups in the military services under NSA operational control; and for submitting recommendations to the Secretary of Defense on ways and means to insure maximum coordination and effectiveness in the overall communications and electronics effort in support of intelligence.

Recommendation No. 3

That more effective technical advice be injected into the USCIB deliberations to permit development of more appropriate statements of the intelligence objectives to be accomplished by communications or electronics means. (See Recommendation No. 1.)

Recommendation No. 4

That the present basic policy for the provision of point-to-point

~~TOP SECRET~~

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

communications services to intelligence community activities from existing governmental or civil communications services be continued. That any attempt to set up separate, duplicate, or paralleling point-to-point communications facilities be authorized only when the necessity therefor has been fully reviewed and agreed to by the Intelligence Communications and Electronics Subcommittee recommended in Recommendation No. 1 above.

Recommendation No. 5

That a basic policy of utilizing existing facilities, services, and equipment to the maximum degree be applied wherever it is determined to be technically feasible in the COMINT, ELINT, and COMSEC operations. This applies particularly to certain aspects of the technical training phases, operational procedures, and logistics. That exceptions to this policy be authorized only when the necessity therefor has been fully reviewed and agreed to by the Intelligence Communications and Electronics Subcommittee recommended in Recommendation No. 1 above.

Recommendation No. 6

That any arrangements with respect to centralized control of ELINT give adequate consideration to the immediate and vital interest of the military in this field and the need to keep electronic countermeasures (ECM) - a tactical weapon - clearly under military operational control.

Recommendation No. 7

That all planning and operation of communications and electronics efforts in support of intelligence activities include full consideration of the following to meet national emergency conditions:

a. Day-to-day operation and training be based on realism in light of the situation and facilities expected to be available in time of war or national emergency. This applies in a special manner to planning

TOP SECRET

operations to be effective in case of heavy jamming operations.

b. Key intelligence installations, served by costly, hard-to-replace electronics equipment and associated records be located outside established target areas. That these installations have integrated plans for national emergency or disaster operations. That all agencies involved in planning new, alternate, or emergency locations for Federal agencies expedite action to assist NSA in its current efforts to obtain a suitable site.

c. Pending accomplishment of b., that effective interim disaster plans be developed promptly for each key intelligence installation to include as a minimum (1) alternate site, (2) installed and tested minimum equipment with necessary basic records at the alternate site, and (3) adequate knowledge of disaster plans by key personnel.

Recommendation No. 8

That the present basic communications (cryptographic) security plan, providing for centralized control with effective decentralization of operations, be continued; that each agency and service maintain effective inspection and vigorous training programs to reduce to the minimum cryptographic operational security violations.

Recommendation No. 9

That NSC determine ways and means to control more effectively release of valuable intelligence to potential enemies via clear text messages being transmitted over government and civil communication networks.

Recommendation No. 10

That the general tendency within the communications intelligence and the communications security agencies to overemphasize the special security facets of their operations with respect to basic communications and

TOP SECRET

TOP SECRET

electronics features be examined objectively and comprehensively by competent, technically qualified authority to insure that such over-emphasis is not producing unnecessary duplication of facilities and operations in peacetime which will grow to completely unrealistic figures in wartime, and producing a system which may fail in an emergency because it will require considerable readjustment of basic operational practices at a critical time. (This service could be accomplished by the subcommittee proposed in Recommendation No. 1 above.)

SPECIAL RECOMMENDATION

THAT THE PRESIDENT SET UP A SPECIAL COMMISSION COMPOSED OF TECHNICALLY QUALIFIED CIVIL AND MILITARY COMMUNICATIONS AND ELECTRONICS REPRESENTATIVES, TO SURVEY AND PRODUCE RECOMMENDATIONS AS TO WAYS AND MEANS TO INSURE THE MORE EFFECTIVE UTILIZATION OF ALL COMMUNICATIONS AND ELECTRONICS RESOURCES OF THE UNITED STATES IN THE NATIONAL INTERESTS IN CASE OF WAR OR NATIONAL EMERGENCY.

During the survey of intelligence activities, it soon became evident that the effectiveness of the whole national intelligence operation was dependent to a high degree on adequate and dependable communications and electronics support, both civil and military. In view of the importance of intelligence operations to the national security, it is important that we know now if these communications and electronics facilities are properly planned, coordinated, and effectively utilized to meet not only peacetime needs, but also anticipated needs likely to develop under the stress of a national emergency. Accordingly, it was determined to make a special survey of the communications-electronics phases of the intelligence activities problem.

TOP SECRET

TOP SECRET

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

Although the time available permitted only a very brief survey of this broad and complex area, the situation appeared to be essentially as follows:

a. Communications and electronics constitute vital means for the collection, transmission, and dissemination of U. S. intelligence in our present worldwide situation. Properly utilized, these means are of high potential value now. As the art develops, the means will increase in potential value.

b. In peacetime, communications facilities and services available to the intelligence activities are considered adequate and reliable. In wartime, it appears that there will not be sufficient communications facilities to meet adequately and dependably all national demands, including intelligence activities. There is need in this area for improvement at high level in coordination and integration of planning for emergency operation. This will involve ^{extensive} coordination between the civil and military operational groups.

c. Operational experience and realistic forecasts of combined communications and electronics requirements for the next national emergency make it abundantly clear now that there are insufficient communications and electronics resources in terms of equipment and trained personnel to meet all these demands. It is imperative that firm plans be developed promptly to insure maximum results from the total communications and electronics resources available.

d. It is important that the communications and electronics means be ready for use when the emergency occurs, rather than sixty to ninety days after the emergency. Again, those responsible for actual civil and military communications are directly involved.

b1a

Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

TOP SECRET

These considerations involve a much wider area of overall national security planning than the intelligence area.

The task force is aware of the report by the President's Communication Policy Board, dated February 16, 1951 (Stewart Report). This was a start on the study of the broad telecommunications problem to develop national policies with respect to effective utilization of radio frequencies, international radio and wire communications, and relationship of government to non-government communications. However, the emphasis appears to be on peacetime planning for development of civil and governmental communications. There is need for more effective relationship of these proposals to emergency conditions.

The task force is also aware that a special advisory committee, consisting of the Director of the Office of Defense Mobilization, the Secretary of State, and the Secretary of Defense, was charged by the President last August with producing information and recommendations on the broad field of U.S. telecommunications by January 31, 1955. As a result, a working party was designated by the Advisory Committee with broad objectives substantially to gather information on the whole telecommunications problem and bring the Stewart report up to date. (No report has been made in response to the January 31, 1955, deadline, and no new target date appears to have been set.) It seems that accomplishment of these broad objectives would not cover the areas envisaged by the Intelligence Task Force. Further, the problem is highly complex and involves technical and operational aspects requiring the consideration and recommendations of the most competent and experienced personnel available in both civil and military communications operations. Members of the present working party do

TOP SECRET

TOP SECRET

not appear qualified to deal effectively with the problem set forth herein.

Information available at the time of the survey indicated that no overall authority has been established at sufficiently high level to deal with this problem within the government departments and agencies, or between government and civil communications agencies. Further, at this time, there is no effective, coordinated guidance of our great civilian communications potential toward preparing to meet officially established national emergency objectives. Such a situation is not good. It reflects the feeling of most Americans over the years that "it can't happen here," rather than a realization that in these days a major disaster can and may happen in our country on very short notice. Lack of firm, well-worked-out national plans, recognized and known by those responsible for the operations, could easily cause a serious breakdown in communications needed to support vital security operations at a critical period. This could directly and adversely affect important intelligence operations.

In view of this situation, this special recommendation with respect to the effective planning for the utilization of our communications-electronics resources in time of national emergency is incorporated in this report.

TOP SECRET

1st Indorsement

To: The Chairman, Commission on Organization of the Executive
Branch of the Government, Washington 25, D. C. May , 1955.

The task force has reviewed with interest Part 2 of APPENDIX I
and concurs with the recommendations contained therein. The need for
adopting the Special Recommendation is especially emphasized; this
is believed to be of great importance.

Mark W. Clark, Chairman,
Task Force on Intelligence Activities

TOP SECRET

XV

ANNEX I

TERMS OF REFERENCE AND COMPOSITION
OF A PROPOSED
INTELLIGENCE COMMUNICATIONS AND ELECTRONICS SUBCOMMITTEE (ICES)
OF THE
COMBINED INTELLIGENCE BOARD (CIB)

Terms of Reference

1. Review and produce recommendations to the Combined Intelligence Board (CIB) with respect to all communications and electronics proposals from intelligence activities which provide for new facilities, equipments, additional personnel, etc., over and above what can be provided from existing resources. The review to include as a minimum consideration of the original intelligence requirements from which the communications and electronics requirements were established, ways and means from the technical viewpoints that the demands might be met. The recommendations should point out which of the essential demands can be met from existing facilities and which should be authorized as additional facilities.
 2. Review operations and produce recommendations to the CIB or furnish guidance directly to operating agencies, to insure that the tendency to overemphasize special security facets in the communications and electronics areas is not producing unnecessary duplication of facilities and operations in peacetime which would grow to completely unrealistic figures in wartime, and is not producing a system which may require considerable readjustment of basic operational practices at a critical time under the pressures of a war or major national emergency.
 3. Make such other technical reviews of communications and electronics operations, plans, or projects related to intelligence as may be requested by the CIB, the Director of Intelligence, or any Central
- Approved For Release 2005/04/22 : CIA-RDP86B00269R000900010001-0

TOP SECRET

department or intelligence agency head.

Composition

1. Communications adviser to the Secretary of Defense (Chairman).
2. Director of the Joint Communications-Electronics Committee of the Joint Chiefs of Staff.
3. Specially qualified ad hoc members to deal with special communications and electronics problems, as agreed by the CIB. They should not be members of an operational activity which has an active interest in the subject under consideration.

Means to Accomplish Tasks

1. To be assisted by qualified individuals or groups in the government service, as arranged by the CIB with departments or agencies concerned.
2. To be authorized special civilian consultants, as the subcommittee may request from time to time to deal with special problems.

TOP SECRET

(Security Classification)



ROUTING			
TO:	NAME AND ADDRESS	DATE	INITIALS
1	C/ISD/OIT		
2			
3			
4			
	ACTION	DIRECT REPLY	PREPARE REPLY
	APPROVAL	DISPATCH	RECOMMENDATION
	COMMENT	FILE	RETURN
	CONCURRENCE	INFORMATION	SIGNATURE
REMARKS:			
FROM: NAME, ADDRESS, AND PHONE NO.			DATE
IRO/DCI			

CONTROL NO.

Cy # 2

Handle Via

COMINT

Channels

Access to this document will be restricted to those approved for the following specific activities:

_____	_____	_____	_____
_____	_____	_____	_____



Warning Notice
Intelligence Sources and Methods Involved
NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions



NOV 3 10 01 AM '80

TOP SECRET

(Security Classification)

DISSEMINATION CONTROL ABBREVIATIONS

NOFORN-	Not Releasable to Foreign Nationals
NOCONTRACT-	Not Releasable to Contractors or Contractor/Consultants
PROPIN-	Caution-Proprietary Information Involved
USIBONLY-	USIB Departments Only
ORCON-	Dissemination and Extraction of Information Controlled by Originator
REL . . .	This Information has been Authorized for Release to . . .

APPENDIX II - CLARK TASK FORCE REPORT

ORIGINAL - DENIED IN 1976/77