

~~U.S. OFFICIALS ONLY~~

~~SECRET~~

**STUDY OF JOINT ORGANIZATIONS
FOR THE PRODUCTION OF
COMMUNICATIONS INTELLIGENCE
AND FOR SECURITY OF
U.S. MILITARY COMMUNICATIONS**

PART B

COMMUNICATION SECURITY

27 DEC. 1948

COPY NO 7

~~SECRET~~

Declassified and approved for release by NSA on 08-22-2013 pursuant to E.O. 13526

~~U.S. OFFICIALS ONLY~~

PART B

STUDY OF A JOINT ORGANIZATION FOR THE SECURITY OF U. S.
MILITARY COMMUNICATIONS

CONTENTS

	<u>Page</u>
Preface	i
I Introduction	1
II Basic Premises	2
III Discussion of Various Arrangements	4
IV Conclusions	13
V Recommendations	13
Navy Comment	15
Air Force Comment	16
Army Comment	17
Appendix "A"	Tab A
Appendix "B"	Tab B
Appendix "C"	Tab C
Appendix "D"	Tab D
Appendix "E"	Tab E
Appendix "F"	Tab F
Appendix "G"	Tab G
Appendix "H"	Tab H
Appendix "I"	Tab I
Appendix "J"	Tab J

~~SECRET~~SECRETP R E F A C E

Complete agreement concerning the organization of a joint or unified armed forces agency for the production of cryptographic materiel and for communications security was not reached. The differences in the view of the Army and Navy members on the one hand, and of the Air Force members on the other, are basically as follows. The Army and Navy members recommend the organization and procedures set forth in Part B. The Air Force members neither support nor reject Part B, but feel that until a decision as to Part A is known, Part B should not be finally acted upon. It is the recommendation of the whole committee, therefore, that Part B should be reviewed subsequently. Withholding final action on Part B is not intended to prejudice parallel actions already in progress for improving coordination in the overall communications security field.

~~SECRET~~

- 1 -

SECRET

~~SECRET~~
~~SECRET~~PART BSTUDY OF A JOINT ORGANIZATION FOR THE SECURITY OF U. S. MILITARY
COMMUNICATIONSI INTRODUCTION

A. In a letter dated 19 August 1948 the Secretary of Defense directed that a committee comprised of representatives of the Army, Navy, and Air Force consider the question, "Should there be Joint or unified Cryptographic Security Activities of the Army, Navy, and Air Force and, if so, What form should they take?"

B. Cryptographic security is only one phase of the field of communication security. A complete consideration of the problem requires consideration of all aspects of the field, which includes, in addition to cryptographic security, transmission security and physical security. The definition of these elements and their relationship to the field of communications are covered in Appendix "A" hereto.

C. Relevant legislation, directives, and basic documents.

1. The National Security Act of 1947 provides for three military departments, each of which has an assigned mission. The act states that in enacting this law "It is the intent of Congress---to provide for their authoritative coordination and unified direction---but not to merge them." Relevant extracts of this act, covering the functions of the Joint Chiefs of Staff, the Munitions Board, and the Research and Development Board are attached hereto as Appendix "B."

2. The Paper Defining the Functions of the Armed Forces and the Joint Chiefs of Staff (Key West Agreement) was approved by the President on 21 April 1948. It sets forth the common functions of all three services and of the Joint Chiefs of Staff. The functions of the departments include the provision that each service will determine and provide the means of communications through which command is to be exercised. Relevant extracts of this paper are attached hereto as Appendix "C."

3. By Executive Order of July 3, 1945 there was created the Cryptographic Security Board, to which are assigned three functions:

~~SECRET~~SECRET

~~SECRET~~~~SECRET~~

- (a) To study and inspect the cryptographic systems and related procedures of all Federal departments and agencies (less FBI).
- (b) To determine and establish cryptographic security standards and policies.
- (c) To promulgate the necessary directives to implement the foregoing.

A copy of this order is attached hereto as Appendix "D."

4. The Joint Chiefs of Staff have established the Joint Communications-Electronics Committee (formerly JCB) as its agency for the coordination of all Joint communications matters. Included within the responsibilities of this committee is that of coordinating Joint communications security matters. The function of making recommendations on communications security matters has been assigned to the Joint Security and Cryptographic Panel of the Joint Communication-Electronics Committee. Copies of the charters of the committee and the panel are attached hereto as Appendix "E" together with a history of Joint Coordination in the field of Communications.

D. Current U. S. Military Communications Security organizations are set forth in Appendix "F."

E. Previous studies have been conducted on the problem of interdepartmental coordination. (See Appendix "G").

F. The results of Joint collaboration in the field of Communication Security are outlined in Appendix "H."

II BASIC PREMISES

A. The communication security problems of the three services, while common in many respects, differ according to the operational mission of each of the services. These problems are outlined in Appendix "I."

B. COMMUNICATION SECURITY is closely related to both communications and intelligence. In the Navy, communication security is considered an integral part of communications. Therefore, the

- 2 -
~~SECRET~~

~~SECRET~~

~~SECRET~~
~~SECRET~~

communication security organization has been made a part of the communications organization, and close Liaison is maintained with the Office of Naval Intelligence. In the Army, the overall responsibility for security has been given to the Director of Intelligence. It is established Army policy to consider communication security as merely one type of security, consequently the communications security organization has been made a part of the Intelligence Division, with liaison with Signal Corps. The Air Force at present depends upon the Army for communication security functions. Their contemplated organization, however, envisages staff supervision by the Director of Communications, in coordination with the Director of Intelligence, who exercises overall control. All three services recognize the need for close liaison between communication intelligence and communication security. This is accomplished in the Army and Navy by putting communication intelligence and communication security under one head, the Chief of Naval Communications in the Navy and the Director of Intelligence in the Army. Air Force plans provide for a single operating organization, directly under the Chief of Staff, to carry out Air Force responsibilities in the fields of communication intelligence and communication security. Although control of this organization will be exercised by the Director of Intelligence, the Director of Communications will exercise staff supervision over all matters pertaining to cryptography and communications security in coordination with the Director of Intelligence.

C. All three services recognize the need for control of communication security functions at general staff level and such control presently exists in each service. The three services differ in the location of this control; in the Navy, control is vested in a communications organization; in the Army, in an intelligence organization; and in the Air Force, in an intelligence organization, working very closely with the communications organization. The Army recognizes the importance of communication security's relation to communications but believes that staff level control is the more important consideration. Army communications are not a general staff function. Therefore the Army is unable to make communication security subordinate to communications within the Army. However, all three services agree that any joint or unified communication security organization must be an integral part of communications and yet must have staff level directive powers.

- 3 -
~~SECRET~~

SECRET

~~SECRET~~~~SECRET~~III DISCUSSION OF VARIOUS ARRANGEMENTS

A. The necessity for joint communication security activities has been presented in the introduction. There are several possible arrangements, including the existing one, through which joint communication security activities probably could be accomplished. These are:

ARRANGEMENT "A."

1. An arrangement whereby each service would be solely responsible for its own communication security. Any matters of joint interest would be settled by means of informal meetings and any agreements reached would be implemented individually by each of the services.

- (a) Although this arrangement was used for many years previous to the activation of the Joint Communications Board (now the Joint Communications-Electronics Committee) and has certain advantages, it is considered to be inadequate to cope with present day requirements and is therefore dismissed without further discussion.

ARRANGEMENT "B."

2. An arrangement whereby each service would be responsible for its own cryptographic security, but where there would be formally established body through which matters of joint interest are coordinated. Meetings would be held at regular intervals and decisions would be reached unanimously before they would be adopted. These unanimous decisions would be implemented by directives issued within each service. Under this arrangement each service would maintain physical means of developing, producing, distributing and accounting for cryptographic aids. Each service also would retain the power to determine communication security doctrine and methods for that service.

- (a) This is the arrangement currently in effect with the Joint Security and Cryptographic Panel of the Joint Communications-Electronics Committee as the coordinating agency; except for the fact that the Air Force does not presently have the means of

- 4 -
~~SECRET~~SECRET

~~SECRET~~
SECRET

producing and handling its own cryptographic material nor of determining its own cryptographic security methods and doctrine, and that the research and development of cryptographic material is within the cognizance of the Research Development Board. Its advantages and disadvantages are discussed below:

(1) Advantages

i Each service retains full command and administration of its own intra-service communication security organization. It is therefore not required to submit to any other service any matters which are not of joint interest. It is also true that intra-service action can be effected more expeditiously unilaterally than by joint action

ii Each service can undertake independent research and development of cryptographic materials and equipment required to carry out its own assigned mission.

iii The facilities of several services can be brought to bear separately on the solution of a single joint problem. Of the several solutions which might be so obtained the best can be chosen.

iv Each service can be equipped and staffed to produce certain joint cryptographic aids for all services. Their personnel can gain experience in the production of these aids, and their plants can be properly equipped for their task.

v No additional high salaried top level administrative personnel are required. Present staffs of the three services can serve on the joint body, thus effecting a saving in personnel and funds.

5
~~SECRET~~

SECRET

SECRET
SECRET

vi Each service can inform the other service of its policies and methods, but can retain within itself information as to specific crypto systems. Thus, it would not be possible for one case of defection to result in the loss of all the cryptographic systems of all services.

vii Since the production facilities of each service are geographically separated, the problem of dispersal is already solved.

viii Since agreements are reached by unanimous consent, each service is fully prepared to carry out its part of the agreement. This might not be true in any arrangement in which a service could be directed to carry out a plan to which it had not given prior agreement.

ix Since the joint body is composed of personnel assigned regular staff duties in their respective organizations, the normal chain of command is followed in reaching and implementing agreements.

x It would be possible to standardize Joint Security policies at the time of their adoption, and to insure their simultaneous implementation.

(2) Disadvantages

1 Under this plan expeditious action on joint matters is not usually effected since time is consumed in reaching unanimous agreement. If joint agreement is not reached, joint action may never be taken.

11 This plan involves the administration and operation of three separate organizations each requiring its own reserves of equipment

- 6 -
SECRET

SECRET

SECRET
SECRET

and staff of administrative, operating, and housekeeping personnel.

- iii No service is required to coordinate its intra-service actions with any other service. In some instances unilateral action might be taken when such should have been a matter of joint cognizance.
- iv There is no requirement to pool abilities and efforts in the research and development field.
- v Implementation of joint agreement is dependent mainly upon joint cooperation, and not upon the exercise of authoritative control.

ARRANGEMENT "C."

3. An arrangement whereby one service would be assigned the responsibility and the means of providing cryptographic security for all services. All other services would contribute funds, personnel and facilities in appropriate amounts. The entire group of personnel and facilities might be concentrated under one roof or in one area or might be physically separated. In any event the entire activity would be the responsibility of one service. This arrangement is not desired by any service because it would not meet service needs effectively in practice.

- (a) This arrangement would require certain budgetary changes by legislation. Responsibility for cryptographic research and development would be delegated to this service subject to the provision of the National Security Act concerning the Research Development Board. Such an arrangement would preclude the necessity for the existence of the Joint Security and Cryptographic Panel of the Joint Communication Electronics Committee. A combined panel would however still be required. Its membership would have to be changed as appropriate to the new organization. The advantages and disadvantages of this arrangement are discussed below:

- 7 -
SECRET

SECRET

SECRET
SECRET

- (1) This arrangement has the following advantages:
- i Insures a single crypto plan for all services.
 - ii Insures positive integration of the communication security equipment requirements and procurement plans for all services.
 - iii Simplifies the control of all the operational details involved in communication security.
 - iv Centralizes physical facilities in a single area or at least, fewer areas than at present, with the result that costs of house-keeping overhead and internal security may be reduced.
- (2) This arrangement has the following disadvantages:
- i Results in a cryptographic plan which might be inadequate to meet the needs of one or both of the other services.
 - ii Could result in the implementation of communication security plans which are biased in favor of the parent service of the security organization charged with the overall responsibility.
 - iii Precludes any exercise of control by the other two dependent services over the security organization of the responsible service. The only recourse of the dependent services would be through their common head - the Secretary of Defense.
 - iv Results in centralization or confinement of physical facilities, consequently increasing the hazard of complete security compromise

- 8 -
SECRETSECRET

SECRETSECRET

through personnel defection or elimination of the entire U. S. military security effort in a concerted attack.

ARRANGEMENT "D."

4. An arrangement whereby a separate organization would be established for the control and direction of the technical, productive, and operating facilities of the three services and for the formulation of basic communication security policies. Under this arrangement each service would have a communication security group physically and administratively independent of the other services but producing material and conducting security activities according to a coordinated plan developed and supervised by the central directive body. The advantages and disadvantages of this arrangement are discussed below:

(a) Advantages

(1) This arrangement has most of the advantages of separate service operating organizations. These briefly are:

i Flexibility of utilization of facilities including rapid action on intra-service matters.

ii Offers a variety of experience and technical capabilities on operating and research and development activities.

iii Dispersed location of facilities.

iv Service administration and supervision of facilities and following of established policies.

v Development of high degree of efficiency which is more possible in a small organization than a large one.

- 9 -
SECRET

SECRET

~~SECRET~~~~SECRET~~

- (2) Rapidity of action after agreement has been reached is assured since under this structure it is not necessary to submit findings to higher authority for approval and promulgation.
 - (3) Standardization at time of formulation and simultaneous adoption and implementation of basic operating security policies.
 - (4) Offers economy of procurement by employment of single contractual action on the bulk of equipment purchased.
 - (5) By establishing control over all basic communication security operating policies, assures that no service can institute any method or communication security policy on an intra-service basis.
 - (6) Provides for pooling of research talent and eliminates possibility for duplication of Research and Development projects by supervision of the research programs of the individual operating agencies.
- (b) Disadvantages
- (1) This plan involves the administration and operation of three separate organizations each requiring its own reserves of equipment and staff of administrative, operating, and house-keeping personnel.
 - (2) Purely intra-service policy decisions are hampered to the extent necessary to submit the action to the joint body for approval.
 - (3) Requires that a body composed of at least three high salaried administrators with appropriate staff be established to meet continuously.

~~SECRET~~

SECRET
~~SECRET~~

- (4) No service could initiate research on a project which had not been assigned to it.
- (5) Competitive service research, providing different solutions for comparison before acceptance, would not be possible.

ARRANGEMENT "E."

5. An arrangement whereby an operating organization directed by communications and security personnel would be established which would be completely responsible for the communication security of all services and which would necessarily operate on the same level as the present Research Development Board or Munitions Board. It would take over the communication security functions and crypto research and development functions of the ASA and CNC. It would have directive power over the services on communication security matters.

- (a) This arrangement would require the enactment of new legislation. It would remove any need for the existence of the Joint Security and Cryptographic Panel. Its advantages and disadvantages are discussed below:

(1) Advantages

- i A single operational organization, providing communications security policy and material, can accomplish its mission without duplicated effort and with a minimum of personnel and facilities.
- ii A single organization would eliminate the necessity for committee action with its accompanying delays. The unanimity problem would no longer be present. Single direction would provide identical procedures throughout the services.
- iii The establishment of a completely unified organization would permit better concentration of effort on security policies and

SECRETSECRET

~~SECRET~~
SECRET

procedures. Rather than have three services making the same security studies a single organization would be able to engage in a greater number of and more extensive studies.

- iv Established at a high level, such an organization would be able to maintain proper and complete control over all security activities throughout the services. Policies would become directives, rather than agreements. Intra-service policies would be the same as joint policies.
- v In the field of research and development all the capabilities of the three services could be utilized toward a common goal. The work could be accomplished without duplication or overlap.
- vi Procurement and allocation of cryptographic material could be handled under a single integrated plan.

(2) Disadvantages

- i Such an arrangement would require a major change in the National Security Act since it does result in a merger which is not the "intent of Congress."
- ii Difficulty might be encountered in channelizing security policies and directives from this organization into the individual armed services.
- iii The services lose freedom of action in communication security matters.
- iv A single case of defection of an employee could result in complete loss of military security.

~~SECRET~~SECRET

~~SECRET~~SECRET

- v A procedure or policy satisfactory in the joint concept might be inefficient from an individual service point of view.

IV CONCLUSIONS

A. It is concluded that:

1. Communication security is but one part, of overall military security. Communication security is an integral part of military communications and of vital interest to intelligence. This is well illustrated in the present day need for ultra-rapid and secure communications - the latter requiring cryptographic devices to be incorporated directly into the transmission circuits as far as possible.

2. Joint control in the highly complex technical field of communication security is necessary.

3. The following characteristics of a joint communication security activity are considered necessary:

- (a) Centralized direction. (and)
- (b) Decentralized, but completely coordinated, implementation.

4. A compromise between arrangement "B" and "D" (outlined in paragraphs III A.2 and III A.4 above) appears to offer an acceptable solution at this time.

V RECOMMENDATIONS

A. It is recommended that:

1. A controlling body composed of communication security experts with a permanent operating staff be established under the JCEC; this group to be known as the Joint Communication Security Panel and to replace the present Joint Security and Cryptographic Panel.

13
~~SECRET~~SECRET

SECRETSECRET

2. This panel be given directive authority, subject to review by the JCEC, over joint communication security matters; it also be given review authority over intra-service communication security matters. For the purpose of this study, the review authority of the panel consists of requiring each service to inform the Joint Communication Security Panel of its intra-service communication security plans for the purpose of determining whether such plans have joint aspects.

3. This panel be given directive authority over production of joint communication security material and review authority over intra-service productive capacity and operations.

4. This panel prepare a coordinated program of communication security research and development for review and approval by the Research and Development Board.

5. There be created a new Cryptographic Equipment Panel, under the Committee on Electronics of the Research and Development Board, with equal representation from each service, utilizing the best qualified personnel of the three services as members.

Note - The formulation of this panel is already in progress.

6. The Joint Communication Security Panel prepare a coordinated program for procurement of communication security equipment (including the industrial mobilization planning necessary to achieve it) for review and approval by the Munitions Board.

7. The Joint Communication Security Panel insure coordination with the Joint Intelligence Committee and/or the United States Communication Intelligence Board whenever matters within the cognizance of those organizations are considered.

8. All directive authority exercised by the Joint Communication Security Panel be subject to review by the JCEC.

9. The United States Air Force maintain a communication security organization adequate to meet Air Force needs.

10. Appendix "J" hereto be adopted as the charter of the Joint Communication Security Panel.

SECRETSECRET

NAVY COMMENT

The Navy is convinced that the problem of Communication Security is so closely concerned with our own military communications that to completely divorce the control of the one from the other would be extremely disadvantageous. The present arrangement, with policy control exercised by the Joint Chiefs of Staff through the Joint Communications and Electronics Committee should be continued but greatly strengthened. With this arrangement, communications and communication security policies are closely integrated and the interests of military intelligence in the overall security field are duly considered by means of intelligence representation on the Communication Security Panel of the JCEC, and by normal internal coordination within each Service.

SECRET~~SECRET~~AIR FORCE COMMENT

The Air Force members recognize the close relationship of Communications Security with both Communications and Communications Intelligence although the members of this Committee have not agreed on all points, they are agreed upon a recommendation for the creation of an Armed Forces Communications Intelligence Board (AFCIB). Such a board would be composed of roughly equal representation from both Communications and Intelligence agencies. It would appear that this might be a convenient body to which jurisdiction could be given for the control of communications security and its proper coordination with the other two functions. There is also the possibility, not yet adequately discussed by the Committee, of requiring the Joint Communication-Electronic Committee and the Joint Intelligence Committee jointly to control Communications Security and to coordinate it with the other two functions. However, since neither fact for the form of AFCIB has yet been determined, it appears impracticable properly to weigh its advantages and disadvantages as a controlling body for Communications Security, against those of the Joint Communications and Electronics Committee. This reasoning forms the basis for the recommendation by the Air Force members that final action on Part B be withheld pending resolution of Part A.

SECRET~~SECRET~~

~~RESTRICTED~~
~~R E S T R I C T E D~~

DEFINITION OF TERMS, AND RELATION
OF CRYPTOGRAPHIC SECURITY TO THE
PROBLEM OF COMMUNICATIONS AS A WHOLE

1. Cryptographic Security is only one phase of the field of Communication Security. A complete consideration of the problem requires consideration of all aspects of the field, which includes, in addition to Cryptographic Security, Transmission Security and Physical Security. These terms are defined in Joint publications as follows:

a. Communication Security: The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from communications.

b. Cryptographic Security: That component of communication security which results from the provision of technically sound crypto systems and their proper use.

c. Transmission Security: That component of communication security which results from all measures designed to protect transmissions from interception and traffic analysis by an enemy.

d. Physical Security: That component of communication security which results from all measures necessary to safeguard classified communications equipment and material from access thereto by unauthorized persons.

2. Since all communications, and especially radio communications, are subject to interception by unauthorized persons, all measures necessary to prevent disclosure of classified information to hostile elements must be employed. In addition to cryptography, some of these measures are:

- (1) Specialized radio equipment, such as beam antennas, Very High Frequencies and Ultra High Frequencies.
- (2) Protected landlines.
- (3) Registration of and accounting for documents and equipment.
- (4) Infra-red transmissions.
- (5) Deception and countermeasures.

~~RESTRICTED~~

~~R E S T R I C T E D~~

~~RESTRICTED~~~~RESTRICTED~~

(6) Monitoring of friendly communication circuits for security supervision.

(7) Radio Silence.

3. Communications is the means by which command is exercised. Effective command whether intra-service or Joint requires that communications be reliable, secure and rapid. Military doctrine requires that the means for communication must be immediately available to a commander, and should be under his direct control.

~~RESTRICTED~~

-2-

APPENDIX "A"

~~RESTRICTED~~

EXTRACTS FROM THE NATIONAL SECURITY ACT OF 1947Declaration of Policy

Sec. 2. In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies and functions of the Government relating to the national security; to provide three military departments for the operation and administration of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force, with their assigned combat and service components; to provide for their authoritative coordination and unified direction under civilian control but not to merge them; to provide for the effective strategic direction of the armed forces and for their operation under unified control and for their integration into an efficient team of land, naval, and air forces.

Joint Chiefs of Staff

Sec. 211. (a) There is hereby established within the National Military Establishment the Joint Chiefs of Staff, which shall consist of the Chief of Staff, United States Army; the Chief of Naval Operations; the Chief of Staff, United States Air Force; and the Chief of Staff to the Commander in Chief, if there be one.

(b) Subject to the authority and direction of the President and the Secretary of Defense, it shall be the duty of the Joint Chiefs of Staff -

(1) to prepare strategic plans and to provide for the strategic direction of the military forces;

(2) to prepare joint logistic plans and to assign to the military services logistic responsibilities in accordance with such plans;

(3) to establish unified commands in strategic areas when such unified commands are in the interest of national security;

(4) to formulate policies for joint training of the military forces;

(5) to formulate policies for coordinating the education of members of the military forces;

(6) to review major material and personnel requirements of the military forces, in accordance with strategic and logistic plans; and

(7) to provide United States representation on the Military Staff Committee of the United Nations in accordance with the provisions of the Charter of the United Nations.

(c) The Joint Chiefs of Staff shall act as the principal military advisers to the President and the Secretary of Defense and shall perform such other duties as the President and the Secretary of Defense may direct or as may be prescribed by law.

Munitions Board

Sec. 213.(a) There is hereby established in the National Military Establishment a Munitions Board (hereinafter in this section referred to as the "Board").

(b) The Board shall be composed of a Chairman, who shall be the head thereof, and an Under Secretary or Assistant Secretary from each of the three military departments, to be designated in each case by the Secretaries of their respective departments. The Chairman shall be appointed from civilian life by the President, by and with the advice and consent of the Senate, and shall receive compensation at the rate of \$14,000 a year.

(c) It shall be the duty of the Board under the direction of the Secretary of Defense and in support of strategic and logistic plans prepared by the Joint Chiefs of Staff -

(1) to coordinate the appropriate activities within the National Military Establishment with regard to industrial matters, including the procurement, production, and distribution plans of the departments and agencies comprising the Establishment;

(2) to plan for the military aspects of industrial mobilization;

(3) to recommend assignment of procurement responsibilities among the several military services and to plan for standardization of specifications and for the greatest practicable allocation of purchase authority of technical equipment and common use items on the basis of single procurement;

(4) to prepare estimates of potential production, procurement, and personnel for use in evaluation of the logistic feasibility of strategic operations;

(5) to determine relative priorities of the various segments of the military procurement programs;

(6) to supervise such subordinate agencies as are or may be created to consider the subject falling within the scope of the Board's responsibilities;

(7) to make recommendations to regroup, combine, or dissolve existing interservice agencies operating in the fields of procurement, production, and distribution in such manner as to promote efficiency and economy;

(8) to maintain liaison with other departments and agencies for the proper correlation of military requirements with the civilian economy, particularly in regard to the procurement or disposition of strategic and critical material and the maintenance of adequate reserves of such material, and to make recommendations as to policies in connection therewith;

(9) to assemble and review material and personnel requirements presented by the Joint Chiefs of Staff and those presented by the production, procurement, and distribution agencies assigned to meet military needs, and to make recommendations thereon to the Secretary of Defense; and

(10) to perform such other duties as the Secretary of Defense may direct.

(d) When the Chairman of the Board first appointed has taken office, the Joint Army and Navy Munitions Board shall cease to exist and all its records and personnel shall be transferred to the Munitions Board.

(e) The Secretary of Defense shall provide the Board with such personnel and facilities as the Secretary may determine to be required by the Board for the performance of its functions.

Research and Development Board

Sec. 214.(a) There is hereby established in the National Military Establishment a Research and Development Board (hereinafter in this section referred to as the "Board"). The Board shall be composed of a Chairman, who shall be the head thereof, and two representatives from each of the Departments of the Army, Navy, and Air Force, to be designated by the Secretaries of their respective Departments. The Chairman shall be appointed from civilian life by the President, by and with the advice and consent of the Senate, and shall receive compensation at the rate of \$14,000 a year. The purpose of the Board shall be to advise the Secretary of Defense as to the status of scientific

research relative to the national security, and to assist him in assuring adequate provision for research and development on scientific problems relating to the national security.

(b) It shall be the duty of the Board, under the direction of the Secretary of Defense -

(1) to prepare a complete and integrated program of research and development for military purposes;

(2) to advise with regard to trends in scientific research relating to national security and the measures necessary to assure continued and increasing progress;

(3) to recommend measures of coordination of research and development among the military departments, and allocation among them of responsibilities for specific programs of joint interest;

(4) to formulate policy for the National Military Establishment in connection with research and development matters involving agencies outside the National Military Establishment;

(5) to consider the interaction of research and development and strategy, and to advise the Joint Chiefs of Staff in connection therewith; and

(6) to perform such other duties as the Secretary of Defense may direct.

(c) When the Chairman of the Board first appointed has taken office, the Joint Research and Development Board shall cease to exist and all its records and personnel shall be transferred to the Research and Development Board.

(d) The Secretary of Defense shall provide the Board with such personnel and facilities as the Secretary may determine to be required by the Board for the performance of its functions.

EXTRACTS FROM THE PAPER DEFINING
THE FUNCTIONS OF THE ARMED FORCES
AND THE JOINT CHIEFS OF STAFF OF

21 APRIL 1948

Section I, paragraph 1:

"1. There shall be the maximum practicable integration of the policies and procedures of the departments and agencies of the national Military Establishment. This does not imply a merging of armed forces, but does demand a consonance and correlation of policies and procedures throughout the National Military Establishment, in order to produce an effective, economical, harmonious, and businesslike organization which will insure the military security of the United States."

Section I, paragraph 2:

"2. The functions stated herein shall be carried out in such a manner as to achieve the following:

(d) Prevention of unnecessary duplication or overlapping among the services, by utilization of the personnel, intelligence, facilities, equipment, supplies, and services of any or all services in all cases where military effectiveness and economy of resources will thereby be increased."

Section II, paragraph B5. - (Common functions of the Armed Forces):

"5. To conduct research, to develop tactics, technique, and organization, and to develop and procure weapons, equipment, and supplies essential to the fulfillment of the functions hereinafter assigned, each service coordinating with the others in all matters of joint concern."

Section II, paragraph B12.

"12. Each service to determine and provide the means of communications by which command within the service is to be exercised."

Section III, paragraph B1. - (Functions of the Joint Chiefs of Staff).

"1. To prepare strategic plans and to provide for the strategic direction of the armed forces, to include the general direction of all combat operations."

Section III, paragraph B2.

"2. To prepare joint logistic plans and to assign to the military services logistic responsibilities in accordance with such plans."

Section III, paragraph B4.

"4. To promulgate to the individual departments of the National Military Establishment general policies and doctrines in order to provide guidance in the preparation of their respective detailed plans."

Section IV - (Functions of the United States Army).

"The United States Army includes land combat and service forces and such aviation and water transport as may be organic therein. It is organized, trained, and equipped primarily for prompt and sustained combat operations on land. Of the three major services, the Army has primary interest in all operations on land, except in those operations otherwise assigned herein."

Section IV, paragraph A1.

"1. To organize, train, and equip Army forces for the conduct of prompt and sustained combat operations on land. Specifically:

- (a) To defeat enemy land forces.
- (b) To seize, occupy, and defend land areas."

Section IV, paragraph A3.

"3. To organize and equip, in coordination with other services, and to provide Army forces for joint amphibious and air-borne operations, and to provide for the training of such forces in accordance with policies and doctrines of the Joint Chiefs of Staff."

Section IV, paragraph A4.

"4. To develop, in coordination with the other services, tactics, technique, and equipment of interest to the Army for amphibious operations and not provided for in section V, paragraph A4 and paragraph A11(c)."

Section IV, paragraph A8.

"8. To develop, in coordination with the Navy, the

Air Force, and the Marine Corps the doctrines, procedures, and equipment employed by Army and Marine forces in air-borne operations. The Army shall have primary interest in the development of those air-borne doctrines, procedures, and equipment which are of common interest to the Army and the Marine Corps."

Section IV, paragraph A9.

"9. To formulate doctrines and procedures for the organization, equipping, training, and employment of forces operating on land, at division level and above, including division corps, army and general reserve troops, except that the formulation of doctrines and procedures for the organization, equipping, training, and employment of Marine Corps units for amphibious operations shall be a function of the Department of the Navy, coordinating as required by paragraph A11(c), section V.

Section V - (Functions of the United States Navy and Marine Corps).

"Within the Department of the Navy, assigned forces include the entire operating forces of the United States Navy, including naval aviation, and the United States Marine Corps. These forces are organized, trained, and equipped primarily for prompt and sustained combat operations at sea, and for air and land operations incident thereto. Of the three major services, the Navy has primary interest in all operations at sea, except in those operations otherwise assigned herein."

Section V, paragraph A1.

"1. To organize, train, and equip Navy and Marine Forces for the conduct of prompt and sustained combat operations at sea, including operations of sea-based aircraft and their land-based naval air components. Specifically:

(a) To seek out and destroy enemy naval forces and to suppress enemy sea commerce.

(b) To gain and maintain general sea supremacy.

(c) To control vital sea areas and to protect vital sea lines of communication.

(d) To establish and maintain local superiority (including air) in an area of naval operations.

(e) To seize and defend advanced naval bases and to conduct such land operations as may be essential to the

prosecution of a naval campaign."

Section V, paragraph A3.

"3. To organize and equip, in coordination with the other services, and to provide naval forces, including naval close air-support forces, for the conduct of joint amphibious operations, and to be responsible for the amphibious training of all forces as assigned for joint amphibious operations in accordance with the policies and doctrines of the Joint Chiefs of Staff."

Section V, paragraph A4.

"4. To develop, in coordination with the other services, the doctrines, procedures, and equipment of naval forces for amphibious operations, and the doctrines and procedures for joint amphibious operations.

Section VI - (Functions of the United States Air Force).

"The United States Air Force includes air combat and service forces. It is organized, trained, and equipped primarily for prompt and sustained combat operations in the air. Of the three major services, the Air Force has primary interest in all operations in the air, except in those operations otherwise assigned herein.

Section VI, paragraph A1.

"1. To organize, train and equip Air Force forces for the conduct of prompt and sustained combat operations in the air. Specifically:

(a) To be responsible for defense of the United States against air attack in accordance with the policies and procedures of the Joint Chiefs of Staff.

(b) To gain and maintain general air supremacy.

(c) To defeat enemy air forces.

(d) To control vital air areas.

(e) To establish local air superiority except as otherwise assigned herein."

Section VI, paragraph A2.

"2. To formulate joint doctrines and procedures, in coordination with the other services, for the defense of the

United States against air attack, and to provide the Air Force units, facilities, and equipment required therefor."

Section VI, paragraph A8.

"8. To develop, in coordination with the other services, doctrines, procedures, and equipment for air defense from land areas, including the continental United States."

Section VI, paragraph A11.

"11. To develop, in coordination with the other services, tactics, technique, and equipment of interest to the Air Force for amphibious operations and not provided for in section V, paragraph A4 and paragraph A11(e)."

A supplement to this agreement dated 21 August 1948 states as follows:-

"Subject to control by higher authority, each service, in the fields of its primary missions, must have exclusive responsibility for programming and planning, and the necessary authority. In the execution of any mission of the armed services, all available resources must be used to the maximum over-all effectiveness. For this reason, the exclusive responsibility and authority in a given field do not imply preclusive participation. In providing for our armed forces, including the preparation of the annual budget and the preparation of mobilization plans, it is essential to avoid duplication and the wastage of resources therefrom. For this reason the service having the primary function must determine the requirements, but in determining these requirements must take into account the contributions which may be made by forces from other services.

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

EXECUTIVE ORDER

CRYPTOGRAPHIC SECURITY WITH RESPECT TO CERTAIN
COMMUNICATIONS OF THE GOVERNMENT

By virtue of the authority vested in me by the Constitution and Statutes as President of the United States, and as Commander in Chief of the Army and Navy of the United States, in order to promote the inviolability of certain Federal communications which affect the national security and interest and in order to promote, through the establishment and enforcement of high and uniform security standards, the inviolability of the cryptographic systems and related procedures utilized to maintain the privacy of such communications, it is hereby ordered as follows:

1. There is hereby created a Cryptographic Security Board (hereinafter referred to as the board); consisting of the Secretary of State, as chairman of the board, and the Secretaries of War and the Navy. The board is charged with the responsibility for the efficient coordination and supervision of all cryptographic systems and related procedures of the Federal departments and agencies. The functions of the board shall be, with the requirements of national security and defense as a primary consideration: (a) to study the cryptographic systems and related procedures of the various Federal departments and agencies, and make periodic inspections and surveys thereof; (b) to determine and establish such cryptographic security standards and policies as will achieve the maximum of security of governmental communications; and (c) to promulgate such directives as may be necessary to implement those standards and policies.

2. The board shall establish a Cryptographic Security Coordinating Committee, consisting of three members, one appointed by the Secretary of State, one an officer appointed by the Secretary of War, and one an officer appointed by the Secretary of the Navy. Such other personnel as may be required to assist the board or the committee in the performance of their functions, may be detailed from those departments in accordance with law. The committee shall perform such of the functions of the board as the board shall direct. The board shall appoint such other committees as may be necessary to carry out its functions. Except as otherwise instructed by the board, committees appointed thereby shall have no power to make final disposition of any

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

matter presented to them by the board for study, but they shall express by written report their findings and recommendations to the board via the Cryptographic Security Coordinating Committee.

3. The board and the committees shall call for consultation such representatives of other government departments and agencies as may be deemed advisable in obtaining full knowledge of the cryptographic matter being studied under the provisions of this order, to the end that the needs of all may be considered and provided for insofar as possible. Other government agencies are directed to cooperate in providing assistance required by the board in its cryptographic studies and to comply with directives promulgated by or on behalf of the board dealing with the use and handling of cryptographic material inside the government establishment.

4. No department or agency shall be required to make available to the board, or to any committee of the board, for use by any other department or agency any cryptographic aid or device, the restricted or exclusive use of which it considers essential to the proper discharge of its duties in the national interest. Nor shall any department or agency be required to disclose to the board or to any of its committees the contents of any official communication concerning its activities if, in the opinion of the head of such department or agency, the disclosure would be contrary to the national interest.

5. The provisions of this order shall not apply to the Federal Bureau of Investigation of the Department of Justice.

6. This order is confidential and shall not be filed in the Division of the Federal Register of the National Archives, or published in the Federal Register, or be given other publicity, until publication thereof has been expressly authorized by the chairman of the board.

(Signed) HARRY S. TRUMAN

THE WHITE HOUSE,

July 3, 1945.

~~CONFIDENTIAL~~**CONFIDENTIAL**

~~RESTRICTED~~~~R E S T R I C T E D~~

HISTORY OF JOINT COORDINATION
IN THE FIELD OF COMMUNICATIONS AND
PERTINENT CHARTERS

1. Early in 1942 the Washington Communications Committee of the interservices Communications Board was established for the coordination of Combined (U.S. - British) communications as well as Joint communications. These committees were later redesignated respectively as the Joint Communications Board and the Combined Communications Board, each of which established committees to deal with communication security matters. The JCB is now known as the Joint Communications-Electronics Committee. Thus, throughout the period since 1942, even prior to the establishment of the Joint Communications-Electronics Committee coordination of all communication matters, including communications security has been effected on both a Joint and Combined basis. The JCEC has established a Joint Security and Cryptographic Panel.

~~RESTRICTED~~~~R E S T R I C T E D~~

~~RESTRICTED~~~~RESTRICTED~~

Tab A

CHARTERJOINT COMMUNICATIONS-ELECTRONICS COMMITTEEORGANIZATION

1. The Joint Communications-Electronics Committee (J.C.E.C.) is the agency of the Joint Chiefs of Staff charged with cognizance of communications and electronics insofar as they pertain to matters for which the Joint Chiefs of Staff are responsible.

MEMBERSHIP

2. The Joint Communications-Electronics Committee shall consist of:

- a. The Chief Signal Officer of the Army.
- b. The Chief of Naval Communications.
- c. The Director of Communications, U. S. Air Force.

3. One or more alternates may be appointed by each member. Whenever a member of the Joint Communications-Electronics Committee is unable to attend a meeting, an alternate will attend as Deputy with plenary powers.

FUNCTIONS

4. The Joint Communications-Electronics Committee is responsible to the Joint Chiefs of Staff to:

- a. Establish joint military policies and plans for communications and electronics systems.
- b. Establish operational characteristics for communications and electronics systems and equipments which may operate interservice. Review and whenever practicable recommend consolidation of military characteristics for communications and electronics systems and equipment for the Armed Services.
- c. Make recommendations to appropriate agencies regarding research and development of communications and electronics systems and equipments.

~~RESTRICTED~~~~RESTRICTED~~

~~RESTRICTED~~~~RESTRICTED~~

d. Based on the Joint Chiefs of Staff strategic concepts, consider major requirements of the several services and unified commands for communications and electronics equipment, and recommend priority of use of available quantities.

e. Determine and allocate to each of the Armed Services, responsibilities in connection with the installation and operation of joint communications and electronics systems, equipments and facilities.

f. Establish joint communications and electronics methods and procedures.

g. Recommend to appropriate agencies the allocation of existing and planned civil communications facilities and systems required by the Armed Services and formulate policy and type agreements with commercial communication companies.

h. Plan military telecommunication frequency requirements. Allocate and coordinate use of emission frequencies for all military equipment. Have cognizance in the matter of preventing electromagnetic interference to all military communications and electronics systems and equipments.

5. The members of the Joint Communications-Electronics Committee shall serve as the United States members of the Combined Communications Board.

PROCEDURE

6. The Joint Communications-Electronics Committee shall:

a. Have the Senior member present act as chairman at committee meetings. If all members should be absent, the senior alternate member present will preside. Otherwise establish its own rules of procedure within the established policies of the Joint Chiefs of Staff.

b. Forward to the appropriate agencies for implementation without reference to the Joint Chiefs of Staff its agreed decisions, except those concerning matters of major policy which will require approval of the Joint Chiefs of Staff.

c. Form panels from personnel of the Army, the Navy, and the Air Force, as required to assist in the performance of its duties. The members of permanent panels will also constitute the U.S. membership on the panels of the Combined Communications Board.

~~RESTRICTED~~

RESTRICTED

7. The Joint Communications-Electronics Committee is authorized to request all Joint Chiefs of Staff, service, and governmental agencies and activities for information and assistance which may be required in connection with its functions and reciprocally, will furnish information and assistance as appropriate to such agencies.

8. The Joint Communications-Electronics Committee, if unable to reach agreement within a reasonable length of time, will submit to the Director of the Joint Staff for submission to the Joint Chiefs of Staff a report indicating where in the members disagree.

Tab B CHARTER OF SECURITY AND CRYPTOGRAPHIC PANEL -
(Membership - 8)

a. Make recommendations regarding the fabrication, employment, distribution and procurement of joint cryptographic systems and equipment.

b. Formulate communication security policies in the following aspects:

- (1) Physical security of publications, documents, equipment and messages.
- (2) Transmission security.
- (3) Cryptographic security.
- (4) The interrelation of operational and communication security.
- (5) Training activities.

c. Make recommendations for the improvement or withdrawal from use of cryptographic systems and equipment as necessary for the maintenance of security.

~~RESTRICTED~~~~RESTRICTED~~

~~SECRET~~~~SECRET~~

CURRENT U. S. MILITARY

COMMUNICATIONS SECURITY ORGANIZATION

1. The U. S. Army - The Army Security Agency is a field activity of the Intelligence Division, General Staff, U. S. Army. The mission of the agency is twofold in that it includes both communication intelligence and communication security. In this study only the Communication Security function is considered. It is subdivided as follows:

a. Research and Development of cryptographic principles and material. All research and development, both Communication Intelligence and Communication Security is carried on by the Research and Development Division at Headquarters, Army Security Agency. The Branches within Research and Development Division which concern themselves with communications security problems are as follows:

- (1) Cryptologic Branch - basic cryptologic research.
- (2) Electro-Mechanical Branch - Design and development of security equipment for telegraph, teletype, authentication and identification communications.
- (3) Ciphony and Cifax Branch - Design and development of security equipment for telephone and facsimile communications.

b. All functions involved in the production and usage of U. S. Army and U. S. Air Force crypto material are carried out by Security Division. These functions are subdivided as follows:

- (1) Compilation, production, storage, accounting and distribution of crypto material is performed by Material Branch.
- (2) Maintenance of crypto equipment and the development and promulgation of maintenance policies and procedures is performed by Maintenance Branch.
- (3) Policies for the employment and procedures for the operation and protection of cryptographic material are formulated and promulgated by the Methods Branch. This Branch also performs continuing cryptanalysis and

~~SECRET~~- 1 -
~~SECRET~~

APPENDIX "F"

~~SECRET~~
~~SECRET~~

critical examination of procedures on U.S. military cryptographic material for the purpose of maintaining a proper evaluation of the security of both.

- (4) Long range planning pertaining to the requirements for and employment of cryptographic material is conducted by the Technical Staff.
- (5) In addition to the cryptographic functions outlined above, analysis of monitored traffic for transmission security violations is conducted by Protective Branch to determine the degree of field compliance with and the suitability of transmission security procedures. This branch also formulates policies and methods for conducting radio deception and countermeasures programs.

c. All budget estimates and justifications are prepared by Army Security Agency and included in the budget of the Signal Corps. The Research and Development program is approved by the Research and Development Group, Logistics Division, General Staff, U.S. Army, and after consolidation with the overall Research and Development program of the Army, by the Research and Development Board.

Army Security Agency procurement is carried on by the Signal Corps, which in turn coordinates its overall procurement program with the Munitions Board.

2. The U.S. Navy - U.S. Navy Regulations direct that all codes and ciphers and signal publications shall be produced by the Chief of Naval Operations. They also provide for the distribution of all registered publications by the Registered Publications Section. In order to meet the requirements of these Regulations the following communications security organization has been established under the Chief of Naval Communications.

a. Research is performed by the Cryptographic research section (Op-204D). This section determines cryptographic principles of U.S. Naval Cryptographic aids and produces laboratory models of any new machines or devices resulting from its research.

b. Engineering Development is carried out by the Naval Code and Signal Laboratory. This laboratory completes

~~SECRET~~~~SECRET~~

APPENDIX "F"

SECRET

engineering on equipment and designs, overhauls and also manufactures in its own shops a considerable portion of the cryptographic machines and devices used in the U.S. Navy.

c. Production of cryptographic devices and machines is a function of the Bureau of Ships (Code 948). The Bureau lets commercial contracts for such equipment or assigns project orders for their manufacture to the Naval Code and Signal Laboratory. Requirements for production are established by the Chief of Naval Communications.

d. The Navy's cryptographic research and development program, and the allocation of funds to support the program is submitted to, and receives approval of the Research and Development Board. The Navy cryptographic procurement program and the allocation of funds to carry it out are approved by the Munitions Board.

e. Production of printed crypto documents is performed for the Navy in the Cryptographic Aids Section (Op-204Y) under the Chief of Naval Communications in the office of the Chief of Naval Operations. Field cryptographic reproduction offices, such as the one at Pearl Harbor, reproduce cryptographic aids for their areas from copy furnished by Op-204Y. Funds for operation of Op-204Y are allocated from Navy Department contingent funds. Funds for Field reproduction offices are allocated by the Bureau of Yards and Docks to the District Commandants.

f. Compilation of Key lists and code vocabularies, the preparation of wiring diagrams and operating instructions is also a function of Op-204Y. Field reproduction offices are not equipped to perform any of these functions.

g. Distribution and Accounting of Registered Publications (which includes cryptographic aids) for the Navy is a function of the Registered Publication System. This system includes the Registered Publication Section (Op-204R) in Washington, and 22 Registered Publication Issuing Offices located throughout the world.

h. Communications Security rules are formulated in The Communication Security Section (Op-204K). This section supervises the operation of the Navy's communication security activities in Washington and in the field, and also determines through its cryptanalytic and traffic analysis subsections, when compromise of Navy cryptographic systems has occurred or is likely to occur.

3. The U.S. Air Force - The Department of the Air Force is engaged in those routine communication security activities organically associated with the operation of its

~~SECRET~~~~SECRET~~

~~SECRET~~SECRET

communications. Unlike the Army and the Navy, the USAF does not have within its present organizational structure, any single agency responsible for directing and coordinating all phases of communication security. However the Departments of the Army and the Air Force are currently negotiating an agreement concerning the transfer of responsibilities for certain communications security activities to the USAF. If the agreement is concluded in its present terms, the USAF will establish a security agency comparable to those presently found within the Army and the Navy.

SECRET~~SECRET~~

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

PREVIOUS AND CURRENT
STUDIES AND PROPOSALS

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

2. An Ad Hoc Committee on the Security of Communications was established on 20 June 1945 by the Joint Communications Board for the purpose of studying the Security of U. S. Intra-Service and Joint Communications. (J.C.B. 174/10/D of 20 June 1945). This committee considered the following joint and intra-service aspects of their problem:

- a. Education.
- b. Terminology and Nomenclature.
- c. Physical Security.
- d. Transmission Security.
- e. Cryptographic Procedures.

3. Correspondence on Research and Development.

On 5 February 1947 Admiral Nimitz (then Chief of Naval Operations) proposed in a Memorandum to General Eisenhower (then Chief of Staff, U. S. Army) that an existing informal Joint Committee to exchange technical information in regard to the Research and Development of crypto-equipment be formalized through their Joint approval. On 23 July 1948, the Army proposed that the research and development of crypto-equipment be placed under the cognizance of the Research and Development Board. On 13 August 1948, the Navy indicated that it did not concur in Research and Development Board cognizance over crypto-equipment and proposed that the charter of the Joint Security and Cryptographic Panel (JCEC) be broadened to include the making of recommendations regarding the research and development of crypto-equipments. The Army has recently reaffirmed its position regarding Research and Development Board cognizance over this subject, but decided not to press the matter over Navy objections. However the Navy later concurred with the Army view in the establishment of a Cryptographic Equipment Panel under the Electronics Committee of the Research and Development Board. This matter has been coordinated with the Air Force.

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

APPENDIX "G"

~~RESTRICTED~~
~~RESTRICTED~~

RESULTS OF JOINT COLLABORATION IN
THE FIELD OF COMMUNICATION SECURITY

1. As a result of collaboration in the communications field, basic doctrine and procedures for Joint Communications have been adopted and published as a series of Joint Communications Instructions. This series has been adopted for intra-service as well as Joint use. (See TAB A hereto). Communication Security has been covered in detail in one of the publications of this series - JANAP 122 "Communication Security."

2. The services have collaborated closely on the contracting and procurement of major items of joint cryptographic equipment. Contracts for crypto-equipment originally intended for one service's use have been expanded to provide for the needs of another service when it became evident that the equipment had joint application. However, joint procurement has not been mandatory.

3. Each Joint cryptographic document is now produced either by the Army Security Agency or the Navy for all three services.

4. In addition to collaboration in production and procurement of cryptographic materials for the National Military Establishment, both the Army and Navy have frequently collaborated in the supply of such materials to other U.S. Government Departments and Agencies and to Allies of the United States.

RESTRICTED

- 2 -
~~RESTRICTED~~

APPENDIX "H"

RESTRICTEDRESTRICTEDLIST OF EXISTING JOINT PUBLICATIONS

<u>JANAP</u>	<u>Long Title</u>
120	Joint Communication Instructions - Forward
121	Joint communication Instructions Part I - General
122	Joint Communication Instructions Part II - Security
123	Joint Communication Instructions Part III - General Procedure
124	Joint Communication Instructions Part IV - Radio Telegraph Procedure
125	Joint Communication Instructions Part V - Radio Telephone Procedure
126	Joint Communication Instructions Part VI - Teletypewriter Procedure
127	Joint Communication Instructions Part VII - Tape Relay Procedure
128	Joint Communication Instructions Part VIII - Facsimile Procedure
129	Joint Communication Instructions Part IX - Visual Procedure
130	Joint Communication Instructions Part X - Direction Finding Procedure
131	Joint Communication Instructions Appendix I - Joint Operating Signals

- 2 -
RESTRICTEDRESTRICTED

TAB "A" to APPENDIX "H"

~~RESTRICTED~~
~~RESTRICTED~~

<u>JANAP</u>	<u>Long Title</u>
132	Joint Communication Instructions Appendix II - Abbreviations
133	Joint Communication Instructions Appendix III - Definitions and Terminology
143	Communication Security
150	Joint Recognition and Identification Instructions - General
151	Joint Recognition and Identification Instructions - Air Force
152	Joint Recognition and Identification Instructions - Ground Forces
153	Joint Recognition and Identification Instructions - Surface Forces
154	Joint Recognition and Identification Instructions - Harbor Defense

RESTRICTED

- 3 -

TAB "A" TO APPENDIX "H"

~~RESTRICTED~~

~~SECRET~~
SECRET

COMMUNICATION SECURITY PROBLEMS
OF THE THREE SERVICES

1. The Naval Communication Service.

a. Four principal types of communications are required by the Navy:

- (1) Between and among the Navy Department, Naval District Commandants, all Naval Stations and the Commanders of Naval operating forces ashore and afloat.
- (2) Between and among ships and aircraft at sea.
- (3) Between ships and aircraft at sea and Coastal Stations.
- (4) Communications for Merchant ships.

b. In meeting these requirements certain basic characteristics of Naval Forces must be taken into consideration. Some of these characteristics are:

- (1) The Navy is a mobile force, most units of which operate for extended periods out of physical contact with the shore establishment and over large distances.
- (2) Because of this fact it is not generally possible to interconnect Naval units by means of landlines. Most Naval communications are dependent upon radio.
- (3) Secure communications must be maintained not only among higher echelons of command, but also down to smaller units, including patrol craft and harbor craft. Such craft are not equipped or staffed to install and maintain complex radio equipment, and must therefore depend principally upon voice equipment for local communications and manually operated C. W. equipment for longer range communications.
- (4) The Naval Cryptographic plan must be designed to meet the security requirements of all echelons and must also suit the limitations of

SECRET

~~SECRET~~ - 1 -

APPENDIX "I"

SECRET
~~SECRET~~

smaller units. It must, in brief, seek to accomplish the following purposes:

- (a) Minimize the effects of capture or compromise. Loss of the entire allowance of a smaller unit should not prevent secure communications among higher echelons. This is the principle of isolation of damage.
- (b) Meet requirements of special situations with special purpose systems (for example: call sign ciphers, authenticators and signal books).
- (c) Provide for privacy within the higher echelons of command.

c. Naval cryptosystems, in order to meet the foregoing requirements and characteristics of Naval communications are organized, distributed and used in accordance with the following plan:

- (1) Cryptochannels - The basic unit for cryptographic communications is known as a cryptochannel. Any flag, ship or station in a given channel can communicate with any other command in that channel.
- (2) Division into Classes - In order to provide the feature of isolation of damage, cryptochannels are organized by echelons of command and types of vessels or stations into seven classes, afloat and ashore. The highest echelon, class 7, is limited to commanders in chief. The lowest, class 1, consists of motor torpedo boats, minor shore activities and smaller craft of the local Naval defense forces. Higher classes hold the publications of all lower classes.
- (3) Segregation by waters - Cryptochannels are segregated on a geographical basis into three areas: Atlantic, Pacific and World-wide.

d. For Merchant ships a series of strip ciphers and running key ciphers have been produced. These are separate from normal Naval Cryptochannels.

~~SECRET~~~~SECRET~~

SECRET
~~SECRET~~

2. The U. S. Army has a two-fold mission involving strategic and tactical defensive and offensive land operations. The communication means (and consequently the communication security means) required to direct combat operations, effect supply, and achieve coordinated strategic planning are different for each.

a. The direction of tactical combat operations requires medium-range, semi-fixed, point-to-point circuits (radio and landline teletype and C. W. circuits) and short range, highly mobile point-to-point, point-to-vehicle, vehicle-to-vehicle, and some air to ground circuits (landline teletype and C. W. and voice radio circuits). The semi-fixed circuits carry traffic of high classification and require cryptographic equipment and procedures which provide long term security and permit rapid, direct, and flexible intra-command communications. The mobile circuits carry traffic usually of medium classification and require cryptographic equipment and procedures which provide relatively short-term security and are practicable for use in vehicles, light planes, or one-man carry. Upon occasion, both types of circuits must communicate with Air Force and Navy operational units.

b. The administration and supplying of land combat and service elements requires long-range fixed and semi-fixed point-to-point circuits (usually teletype and C. W. radio and landline teletype circuits). These circuits carry traffic of high classification and require cryptographic security equipment and procedures which provide long term security and permit communication with departmental and tactical organizations.

c. The achievement of coordinated strategic planning requires long-range, fixed, point-to-point circuits (usually radio teletype circuits). These circuits carry traffic of the highest classification and require cryptographic equipment and procedures which provide exceptionally long-term security and permit intercommunicability with major commands of all three services.

d. In addition to the communication security problems imposed by the divergent types of communications listed above, there are such special problems as the provision of security equipment for military attaches, communication intelligence units, U. S. Army transports, various non-military agencies of the government, and military services of certain foreign nations.

e. Finally, the development of militarily practicable facsimile television and pulse-code modulated equipment requires

~~SECRET~~3 -
~~SECRET~~

APPENDIX "I"

~~SECRET~~
~~SECRET~~

the development of special security equipment in order that these new communications means may be used for handling classified information.

3. Air Force.

a. The primary mission of opposing the enemy with our air potential has been assigned to the USAF. This mission has been divided into several major phases with responsibilities charged as follows:

- (1) Bombardment of strategic targets is the responsibility of the Strategic Air Command.
- (2) The support and protection of ground elements is the responsibility of the Tactical Air Command.
- (3) The air defense of the continental United States is the responsibility of the Air Defense Command.
- (4) The transport mission is the responsibility of the Military Air Transport Service.

b. In order to execute the phase of the USAF mission for which it is responsible, each of these commands is dependent upon numerous and varied types of communications:

- (1) The Strategic Air Command requires long range radio teletype, CW and voice, communications in order to control the deployment of large masses of aircraft engaged in trans-hemispheric operations.
- (2) In order to move masses of troops and ground equipment, well coordinated air coverage must be furnished if ground forces are to be protected from enemy air forces to which they may be exposed. In order to effect this coordination of air-ground cooperation the Tactical Air Command must place extensive reliance on short range, rapid voice communications.
- (3) In effecting air surveillance over targets in the United States, the Air Defense Command employs a complex system of early radio warning nets linked by voice and teletype com-

SECRET

~~SECRET~~

~~SECRET~~
SECRET

munications required for the plotting of timely intercept of attacking enemy air units and guided missiles. The keynote of these communications must be utmost speed and reliability.

- (4) The Military Air Transport Service, in discharging its responsibilities for supporting all of the services with air lift to bases throughout the world is dependent upon a vast net of linking communications for the rapid flow of logistical data, flight information, and the collection and dissemination of weather forecasts necessary for its operations as well as those of other air force units.

c. The intelligence available to this service as regards the efforts which the Axis Nations exerted during the last war on all types of Air Force communications poignantly illustrates the vulnerability of air communications to hostile intrusion. The Japanese as well as the Germans enjoyed singular success in exploiting Air Force communications which were especially productive of intelligence because of the Air Force requirement for transmitting much interrelated information over both point-to-point communication and air-ground communication channels.

d. While the U. S. Air Force is intensely aware of the shortcomings in its communications which make them interesting targets for hostile intercept organizations, it has not been possible in the short time since the end of World War II to produce radically improved equipments to replace those upon which it relied for security of our communications during the war. Presently existing crypto machines, although possessing considerable inherent security, are not geared to the speed of operation which must be provided. High-echelon manual crypto-devices do not meet the requirement for cryptographed communications over USAF radio teletype circuits. The transmission of weather maps by facsimile cannot be protected as yet with efficient secure crypto elements. Adequate methods of meeting the voice security requirements of the USAF have not been achieved. Dangerous amounts of air order of battle information would be available in the event of war by the traffic analysis of channels carrying flight movement messages, even without regard to the security of any present type cryptosystems which might be employed.

~~SECRET~~~~SECRET~~

~~RESTRICTED~~
~~RESTRICTED~~

PROPOSED CHARTER

FOR THE JOINT COMMUNICATIONS SECURITY PANEL

(Membership 9, three from each service)

1. Formulate joint, and review intra-service, communication security policies in the following aspects:

- a. Physical security.
- b. Transmission security.
- c. Cryptographic security.
- d. The interrelation of operational and communication security.
- e. The interrelation of communication security and communication intelligence.
- f. Communication cover plans.
- g. ,Training activities.

2. Subject to the review of the JCEC, direct the fabrication, distribution and employment of joint communication security documents, systems and equipments. Review and make recommendations regarding the same aspects of intra-service communication security documents, systems, and equipment. For the purpose of this charter, review by the panel means that each service is required to inform the panel of its intra-service communications security plans for the purpose of determining whether such plans have joint aspects.

~~RESTRICTED~~

~~RESTRICTED~~

~~RESTRICTED~~~~RESTRICTED~~

3. Make recommendations for the improvement or, subject to the approval of the JCEC, direct the withdrawal from use of cryptographic systems and equipment as may be dictated by security requirements.

4. Prepare for review and approval by the Research and Development Board, a coordinated program for research and development of U. S. Military communication security equipment, and when approved take action to implement this program.

5. Prepare for review and approval by the Munitions Board, a coordinated program, including industrial mobilization planning, for the procurement of U. S. Military communication security equipment, and when approved take action to implement this program.

6. Insure coordination with the Joint Intelligence Committee whenever policy considerations are involved affecting operational security.

7. Insure coordination with the United States Communication Intelligence Board whenever policy considerations are involved affecting communication intelligence.

8. When no change in Joint Communications or Joint Intelligence policy is involved, the Chairman will prescribe appropriate action to implement unanimous Panel decisions concerning Joint communication security and/or cryptographic

~~RESTRICTED~~~~RESTRICTED~~

~~RESTRICTED~~

matters under cognizance of this Panel, in accordance with this charter, and will promptly furnish each of the Heads of the Communications and Intelligence branches of the three Services with a copy of all directives thus issued - for implementation by each Service.

9. The Chairmanship of this Panel shall be rotated once annually among the three Services in the order of Service seniority, with the Head of the Communications or Intelligence branch, as appropriate in each service, nominating the person to be Chairman from among its members on the Panel.

~~RESTRICTED~~~~RESTRICTED~~