Mr. Brann -

This is the carbon for file which I spoke to you about.

Mrs. Pyper

~~SECRET~~

File "Development"

Copy for AS-80

5 AS-23 AS-14 23 May 47

1. Attached hereto is final draft of material recommended for inclusion in the War Department Research and Development Program for FY 1949. Concurrences have been obtained from AS-70, 80 and 90.

3 Incls.
Added 1 incl
3. Draft of Section
XIV, "Communications
Security Equipment."

WILLIAM F. FRIEDMAN
Chief, Communications Research
Extension 215

~~SECRET~~

SECRET

DRAFT

SECTION XIV

COMMUNICATIONS SECURITY EQUIPMENT

ASSIGNMENT OF PRIMARY COGNIZANCE

Primary cognizance for research and development in the field of communications security equipment is assigned to the Director of Intelligence. Responsibility for projects, where the security element is an integrated portion of an item of communications equipment being developed by the Signal Corps, rests with the Chief Signal Officer. However, coordination with the Director of Intelligence through the Chief, Army Security Agency is required in connection with the security features of such integrated equipment.

STATUS OF PRESENT TECHNICAL KNOWLEDGE

1. Technical knowledge applicable to the field of communications security has advanced considerably beyond its status during the War. These advances are the result of extensive War Department research and development both in cryptographic methods and in associated engineering techniques. General scientific advances have made possible the design of security equipment compatible with future planned communications systems.

2. New developments in communications methods and techniques and new applications of such developments in the Army, have resulted in new Basic Military Requirements for communications security equipment. For

SECRET

many of these new requirements, the general approach to the fulfillment of these requirements is known. However, the provision of the ultimate in communications security equipment for each communications need will require considerable research and development.

3. The long-range research and development program is dependent upon basic research into applicable electrical phenomena, cryptologic principles, highly specialized electronic tubes and other electronic techniques, as well as the development of specialized components which can be applied to a number of developmental projects.

4. Active liaison with other governmental agencies and with commercial firms is being maintained to insure that early application is made of scientific advances or extensions thereof.

SUMMARY OF PRESENT PROJECTS

1. Communications Security Equipment Development is based on requirements submitted as M/C's by the Army Ground Forces and the Army Air Forces as well as requirements of high echelons of the War Department. These requirements as well as Army Security Agency estimates of future requirements are coordinated into a basic Cryptographic Plan of which the development program is a part. This program planning is directed to provide all the using forces of the Army with secure and operationally practicable cryptographic mechanisms for each means of communications, and at the same time reducing to a minimum the number of types of security equipment required.

2. Communications Security Equipment under current development will satisfy requirements for communications of the following categories:

a. Ground Point-to-Point Communications (covers both short and long range)..

b. Air-to-Air and Air-to-Ground Communications.

c. Specialized Communications (includes authentication systems, weather systems, map reference systems, etc.).

These categories include any established means of communication, such as wire and radio, employed by the United States Army. Research and development is closely coordinated with current plans of the using echelons, including adaptability of the equipment to operation in integrated communication systems. Policies of design and operation closely parallel the trends of communications equipment itself. This includes reduction in size and weight by use of sub-miniature components, development of special components as required, and by research into electronic engineering and cryptologic techniques which will effect substantial reductions. Development efforts are directed toward effecting a minimum of moving mechanical parts, elimination of multiplicity of different components and the incorporation into equipment of packaged sub-assemblies in order to improve performance, to simplify maintenance and replacement, and to provide training "editions" in forward echelons. In addition, initial research is being conducted on the problems of providing security for television and for communication systems employing ultra high frequencies.

3. The categories listed in Paragraph 2 above include equipment which will provide for the following methods of communication:

a. Off line literal communications.

b. Teletype communications.

c. Voice communications.

d. Facsimile

present, particular emphasis is placed on items (b) and (c), with priority being given to mechanisms for low echelons based upon specific requests from Air and Ground Forces.

4. A program parallel to that for providing communications security equipment is conducted in the field of Communications Intelligence. Research and development of principles and equipment for intercepting and recording all types of communications, including new methods as they appear, is a continuing problem of major proportions. Extensive research into new cryptanalytic principles and the development of associated equipment for the application of these principles constitute an active portion of the program. This work must be vigorously pursued in order to be able to cope with new communication methods resulting from scientific advances in the field.

FUTURE RESEARCH AND DEVELOPMENT

1. A very considerable amount of research will be required to satisfy existing requirements for Communications Security Equipment. New cryptographic principles must be discovered. Engineering techniques must be developed which will embody these principles and at the same time operate in conjunction with existing communications equipment or equipment under development. In the development of communication security equipment it is frequently possible to employ techniques and components which are the result of general scientific advancement. However, much of the knowledge required is peculiar to the specific equipment involved and therefore must be obtained by special research. At the present state of the art, security equipment frequently requires more exacting design and conditions of usage than the associated communications equipment. The progress of other governmental, commercial, and university scientific

research and the extent of this research will govern a portion of future research directed toward the development of security equipment.

2. Each new type of Communications Equipment or new method of using Communications Equipment which is adopted by the Army establishes a requirement for a new type of security equipment. As these new requirements arise they present the necessity for new projects for cryptographic research and related engineering research. Development of security equipment for facsimile and television communication will parallel development elsewhere in the Army of the means for providing these communications.

3. The problem of providing Communications Security is a continuously active problem. Cryptanalytic advances are always attempting to overtake cryptographic techniques. Therefore if there is not a continual advancement in cryptographic techniques which take advantage of the most advanced achievements in the field of science, the security of communications will be placed in serious jeopardy. It is therefore necessary that the Army continue a concentrated research program to provide new and better cryptographic principles which utilize the best that technological advances can provide.

FISCAL INFORMATION

1. Total funds carried over from previous Fiscal Years ...$ 431,262

2. Appropriation for Fiscal Year 1947 1,818,000

3. Appropriation approved by Bureau of Budget for Fiscal Year 1948 2,206,780

4. a. Estimated total ultimate cost of projects for which an item can be foreseen but not including the cost of continuing projects 5,454,000

   b. Estimated total annual cost of continuing projects; i. e., those projects for which no end item or termination can yet be foreseen 906,000