COPY

~~SECRET~~ ID:A60954

1. AS-14 AS-23 9 May 47 Comment Regarding ASA Research and Development Activities for Inclusion in War Department Research and Development Program, Fiscal Year 1949

Major Bergman/462

1. Reference is made to attached copy of Comment No. 3 of Disposition Form to Chief, Training Group, which indicates that this Agency will supply a comment covering Army Security Agency research and development activities for inclusion in the War Department Research and Development Program, Fiscal Year 1949.

2. It is desired that this comment be prepared by your office and that it be submitted to this office by 16 May 1947. Necessary coordination will be effected with AS-70, 80, and 90 prior to submission.

3. The comment should not contain any information which bears a classification higher that SECRET or which will require that the recipients thereof be cryptographically cleared.

4. Attached for your information is the document, War Department Research and Development Program, Fiscal Year 1947, which illustrates the desired type of comment relating to the research and development activities of the Army Security Agency. It is desired that this document be returned with your recommended comment.

2 Incls
1. Cy Disp Form, subj: Supplement to FY 1948 Research & Development Program
2. WD Res & Dev Program, FY 1947

/s/ Paul E. Neff
for GEORGE.A. BICHER
Colonel, Signal Corps
Deputy Chief, Army Security Agency
Ext 498

---

2. AS-70 AS-14 12 May 47 1. Attention is invited to Comment No. 1 above together with attached inclosures. It is requested that a draft for an ASA Section in the WD Research and Development Program for FY 1949 be prepared, using as a guide the FY 1947 Program. Wording of draft should not be hampered because of security reasons, since it will be reworked later to bring it down to the SECRET classification in coordination with AS-80 and AS-90.

2. Please note deadline date given AS-14 for completed paper (16 May).

2 Incls
n/c

/s/ Mark Rhoads
for WILLIAM F. FRIEDMAN
Chief, Communications Research
Ext 215

~~SECRET~~

COPY

3. AS-14 AS-71 14 May 47 Comment Regarding AS Research and Development Activities for Inclusion in War Department Research and Development Program, Fiscal Year 1949

1. Reference is made to Section XIV of War Department Research and Development Program for Fiscal Year 1947, Subject; Communications Security Equipment. It is recommended that the contents of the draft for Fiscal Year 1949 be substantially the same as that contained in this reference. In order to conform with the arrangement contained in the program for Fiscal Year 1948, it is necessary that the item on "Assignment of Primary Cognizance" be listed first and that an item on "Fiscal Information" be added.

2. In order to bring the statements for the Fiscal Year 1947 program up to date, it is recommended that the following changes or additions be made:

a. "Assignment of Primary Cognizance" should be revised to read as follows: "Primary cognizance in this field is assigned to the Director of Intelligence. Responsibility for projects, where the security element is an integrated portion of an item of communication 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."

b. "Status of Present Technical Knowledge"

(1) Paragraph 1 should be revised to read as follows: "Technical knowledge applicable to the field of communications security is considerably advanced in comparison to its status during the war. These advances were 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 equipment which was needed earlier in the war but was not available. The long range development program is dependent on basic research into applicable 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 development projects. Active liaison with other governmental agencies and commercial firms has made possible the early application of scientific advances or extensions thereof."

(2) The last sentence of Paragraph 2 should be revised to read as follows: "This work is mainly in the fields of radio and wire communications but also includes any other currently used or proposed methods of communication."

c. "Summary of Present Projects"

(1) The last portion of Paragraph 2 should be revised to read as follows: "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

3. AS-14 AS-71 14 May 47

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 and to simplify maintenance and replacement in forward echelons."

(2) The following should be added to Paragraph 2: "In addition, initial research is being conducted on the problems of providing security for television and for communication systems employing ultra high frequencies."

d. "Future Research and Development"

(1) Add to Paragraph 1: "At the present state of the art, security equipment generally requires more exacting design and conditions of usage then the associated communications equipment. The progress of other governmental and commercial scientific research and the extent of this research will govern a portion of future research directed toward the development of security equipment."

(2) Add to Paragraph 2: "Development of security equipment for facsimile and television communication will parallel development elsewhere in the Army of the means for providing these communications."

e. The following should be added to complete the Section "Fiscal Information."

1. Total funds carried over from previous Fiscal Years.....$ 431,262
2. Appropriation for Fiscal Year 1947..... 2,018,000
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 end 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

/s/ S. Kullback
S. KULLBACK
Chief, RL Div.
Ext 321

To AFSAC 5/19/47

Comment Regarding ASA Research and Development Activities for Inclusion in War Department Research and Development Program, Fiscal Year 1949 (contd)

4. AS-14 AS-80 19 May 47

1. It is considered that the Communications Security Equipment Section (Section XIV) of the War Department Research and Development Program, Fiscal Year 1949, should be presented in a form similar to the attached draft. Cognizance has been taken of the recommendations of Research Laboratories Division as shown in Comment Number 1.

2. It is recommended that further coordination with WDGAS-70 and WDGAS-90 be effected.

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

A. SINKOV
Chief, Security Division
Extension 241

20-17110 37

Daily file

Sig

~~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 many of these new requirements, the general approach to the fulfillment of these

~~SECRET~~

Incl 3

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. The possibility is being considered of arranging for research on related problems to be carried out in academic institutions.

SUMMARY OF PRESENT PROJECTS

1. Considerable effort is being directed toward the preparation of a Cryptographic Plan to serve as a guide for the future research and development program in the field of communications security equipment. The object of such a program is to provide the using forces of the Army with secure and operationally practicable communications security equipments for every communications need.

2. In the Cryptographic Plan the communications security requirements of the Army are considered under three 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.).

3. Predicated upon the class of the using agency, the means of communication available to those agencies, and certain fundamental principles desired for cryptographic mechanisms and systems, the Cryptographic Plan establishes the Basic Military Requirements which must be fulfilled by communications security equipments provided to meet each communications need, and lists these Basic Military Requirements under each of the three categories of communications.

4. Coordination has been effected with the Army Ground Forces and the Army Air Forces, who have presented sets of Military Characteristics which they desire specific items of communications security equipment to possess to meet their communications needs. These Military Characteristics have been related to the Basic Military Requirements listed under each category of communications.

5. Communications security equipments required under the Cryptographic Plan include equipments which provide security for the following methods of communication:

a. Facsimile communications.

b. Teletype communications.

c. Voice communications.

d. Off-line literal communications.

Based upon expressed desires of the Army Ground Forces and the Army Air Forces, priority is being given at the present time to the development of small, light-weight communications security devices which will provide security for teletype and voice communications in the lower echelons.

6. Research and development of communications security equipment is proceeding, therefore, upon the basis of firm requirements and priorities as expressed by the using forces, and is being closely coordinated with current and future plans of the using echelons, including adaptability of the equipment to operation in integrated communications 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 such reductions. Development efforts are directed toward effecting a minimum of moving mechanical parts, elimination of multiplicity of different components and the incorporation into the equipment of packaged sub-assemblies in order to improve performance and to simplify maintenance and replacement in forward echelons.

7. Initial research is being conducted on the problems of providing security for television and communications systems employing ultra-high frequencies.

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 communications 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.

2. Each new type of communications equipment or new method of using communications equipment which is adopted by the Army requires the provision of a new type of security equipment. As these new requirements arise, they necessitate the establishment of new projects for cryptographic research and related engineering research.

3. The provision of communications security is a continuously active problem. Advances in cryptanalytic methods are always striving to weaken communications security, and only by continual improvement in cryptographic principles and techniques can the security of communications be assured. It is necessary, therefore, that the Army pursue a vigorous research program to discover and employ new and stronger cryptographic principles and techniques which will assure the continuing security of United States Army communications.

FISCAL INFORMATION

1. Total funds carried over from previous Fiscal Years ..... $ 431,262
2. Appropriation for Fiscal Year 1947..... 2,018,000
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 end 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