



dir

CONFIDENTIAL
NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

Serial: N 4702
 29 NOV 1960

~~CONFIDENTIAL~~

MEMORANDUM FOR THE DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING

SUBJECT: Draft Department of Defense Instruction, Subject: "Policies and Procedures for Communications Security Research and Development (U)

1. On 7 November 1960 the following personnel met to discuss comments on the subject Instruction forwarded to DDR&E by the Secretaries of the Military Departments:

| | |
|-------------------------|-----------|
| Mr. H. Stadermann | DDR&E |
| Mr. D. Wolfand | NSA |
| Lt Col J. Anderson, USA | NSA |
| Lt Col L. Brownfield | OCRD, USA |
| Mr. R. Scott | OCSigO |
| CAPT R. Cook | NSG |
| Mr. J. Boyd | NSG |
| Maj D. Nowakoski | ARDC |

2. All differences were resolved and the following agreed to by those present:

- a. Early publication of the document is essential.
- b. The new draft would not require a second review by the Secretaries. Instead, the normal review by the Armed Forces Policy Council would suffice.
- c. Coordination with the Administrative Assistant to Secretary of Defense would be required to approve the existence of CREC. This coordination would be accomplished by Mr. Stadermann.

3. A new draft of the subject Instruction dated 16 November 1960 and revised in accordance with the resolution of comments from the

Declassified and approved for release by NSA on 10-28-2013 pursuant to E.O. 13526

~~CONFIDENTIAL~~

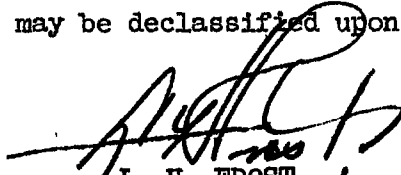
~~CONFIDENTIAL~~

Serial: N 4702

~~CONFIDENTIAL~~

Secretaries of the Military Departments, is forwarded for appropriate action in accordance with agreements outlined in Paragraph 2.

4. This correspondence may be declassified upon removal of the Inclosure.



L. H. FROST
Vice Admiral, USN
Director


Incl:
a/s (6 cys)

Copy Furnished:
General G. B. Erskine, USMC-Ret,
Asst to SecDef, Sp Opns (2 cys of Incl)

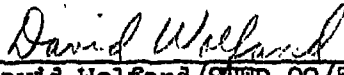
JCS (J-6)
Head, NSG (2 cys of Incl)
OCSigO (3 cys of Incl)
Hq, USAF, DCS/Development (2 cys of Incl)

~~CONFIDENTIAL~~

Serial: N 4702

cc: DIR 
AG
Reading File
R/D Reading File
CSEC-04 (2 cys of Incls)
R/D-02
SIED-02 (2)

M/R: Draft Department of Defense Instruction, Subject: "Policies and Procedures for Communications Security Research and Development" has been revised in accordance with resolution of comments obtained from Secretaries of the Military Departments by DDR&E. Attached correspondence forwards revised draft to DDR&E for further coordination in DOD and with Armed Forces Policy Council. Coordinated with CSEC-04 (LtCol J. Anderson).



David Wolfand/SIED-02/5114/pml/16 Nov 60

CONFIDENTIALCONFIDENTIALDRAFT

16 November 1960

DEPARTMENT OF DEFENSE INSTRUCTION

SUBJECT: POLICIES AND PROCEDURES FOR COMMUNICATIONS SECURITY
RESEARCH AND DEVELOPMENT (U)

- References: (a) Department of Defense Directive C-5200.5, Subject: "Communications Security (COMSEC)", dated 27 Oct 1958
- (b) Department of Defense Directive S-5100.20, Subject: The National Security Agency, dated 19 March 1959

I. PURPOSE AND SCOPE

1. This Instruction establishes policies and procedures concerning Communications Security (COMSEC) research and development within the Department of Defense. These procedures encompass the aspects of (1) generalized and detailed requirements and determination of Joint interest, (2) program development-budget presentation and (3) program implementation, review and control. In establishing such policies and procedures it is the intent that they be of benefit to the Military Departments and the Director, NSA in their mutual endeavor to attain the objectives of the Secretary of Defense as outlined in Section III of reference (a) as these concern cryptosecurity research and development. These procedures are further intended to enable the Director, NSA to discharge his responsibilities (reference (b)) in connection with the COMSEC research and development portion of the Department of Defense cryptologic program.
2. Maximum mutual benefit cannot be derived by adherence only to set procedures. It is considered highly desirable for Senior COMSEC personnel of NSA and the Services to convene as required for formal discussion of

Incl~~CONFIDENTIAL~~

~~CONFIDENTIAL~~~~CONFIDENTIAL~~DRAFT

NSA-Service COMSEC R&D problems. Furthermore, it is considered essential that a continual exchange of COMSEC R&D information be effected primarily, but not exclusively, via an NSA-Services COMSEC Research and Engineering Committee (CREC).

II. DEFINITIONS

The following definitions apply herein:

1. Research and Development (R&D) - Includes research, development, testing, evaluation and engineering occurring in a period which begins with the initiation of a project, and which ends with the project termination or completion of user tests, whichever is earlier.
2. COMSEC - The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study. Communications security includes: (1) transmission security, (2) cryptosecurity, and (3) physical security of communications security materials and information.
 - a. Transmission Security - Transmission security is that component of communications security which results from all measures designed to protect transmission from unauthorized interceptions, traffic analysis, and imitative deception.
 - b. Cryptosecurity - That component of communications security which results from the provision of technically sound cryptosystems and their proper use.
 - c. Physical Security - That component of security which results from

~~CONFIDENTIAL~~

CONFIDENTIALCONFIDENTIALDRAFT

all physical measures necessary to safeguard classified equipment, material and documents from access thereto or observation thereof by unauthorized persons.

3. COMSEC Equipment - Equipment designed to provide security to telecommunications during transmission by converting information to a form which is unintelligible to an unauthorized interceptor and by reconverting to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment is crypto-equipment, crypto-ancillary equipment, cryptoproduction equipments and authentication equipment.
 - a. Crypto-equipment - Any COMSEC equipment which converts information for transmission to a form which is unintelligible to an unauthorized interceptor, or which reconverts such information to its original form for authorized recipients.
 - b. Crypto-ancillary equipment - Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment but which does not perform any of the functions of crypto-equipment, and equipment designed specifically to convert information to a form suitable for processing by crypto-equipment.
 - c. Cryptoproduction equipments - Equipments, and components thereof, that are specifically designed for, and used in the manufacture and associated testing of COMSEC materials.
 - d. Authentication equipment - Equipment designed to provide protection against fraudulent transmissions or to establish the authenticity of a message or communication system.

CONFIDENTIAL

~~CONFIDENTIAL~~~~CONFIDENTIAL~~DRAFT

4. Cryptomaterial - All material, including documents, devices and/or equipment or apparatus essential to the encryption, decryption or authentication of telecommunications.
5. Cryptoprinciple - The characteristics of the elements involved in, and the fundamental rule of operation, motion or activity inherent in a cryptosystem.
6. Cryptosystem - The associated items of cryptomaterial which are used as a unit and which provide a single means of encryption and decryption.

III. CRYPTOMATERIAL R&D REQUIREMENTS AND DETERMINATION OF JOINT INTEREST - See Appendix I.

IV. PROGRAM FORMULATION - BUDGET PRESENTATION - See Appendix II.

V. PROGRAM IMPLEMENTATION, REVIEW AND CONTROL - See Appendix III.

VI. CLASSIFICATION

This document may be reproduced in whole or in part for convenience in implementation. For appropriate protection, the paragraphs of the document which are classified are so identified. The classification of the various portions of the Instruction is as follows:

1. Cover document - Unclassified, FOR OFFICIAL USE ONLY.
2. Appendix I - Unclassified, FOR OFFICIAL USE ONLY.
3. Appendix II - Unclassified, FOR OFFICIAL USE ONLY.
4. Appendix III - CONFIDENTIAL

VII. EFFECTIVE DATE - The effective date of this Instruction is _____ 1960.

~~CONFIDENTIAL~~

DRAFTAPPENDIX ICRYPTOMATERIAL R&D REQUIREMENTS AND DETERMINATION OF JOINT INTEREST

I. RESPONSIBILITIES

It is the responsibility of each Service to determine its own needs for the application of COMSEC in connection with (its own) separate communications means---communications systems, terminal equipments and transmission means---and in connection with communications means which are a part of a "weapons" system or other electronic system. It is also the responsibility of the Military Departments to formulate and submit to the Director, NSA long-range generalized and more detailed current cryptomaterial R&D requirements. Responsibilities for determination of need for application of COMSEC to a Joint or common DOD communications system will be assigned when directives for such a system are published. The Director, NSA is charged with the responsibility for formulating long-range R&D plans and integrated R&D programs to ensure (the existence of a capability for) the security of military telecommunications. The requirements submitted to the Director, NSA thus form the basis for the above-mentioned plans and programs.

II. OBJECTIVES

1. Long-range generalized cryptomaterial R&D requirements are those in which the Services describe a need, in the form of objectives, for various cryptosecurity means to be associated with planned means of communications. The more detailed cryptomaterial R&D requirements are formulated as the communications art matures and funds become available to implement the development of planned communications means. These detailed cryptomaterial

DRAFT

APPENDIX I

R&D requirements may be described, for example, in the form of an operational requirement (OR), Operational Support Requirement (OSR), General Operational Requirements (GOR), Qualitative Material Requirement (QMR) and military (MC) or development characteristics (DC).

2. The availability of consolidated, up-to-date long-range cryptomaterial R&D requirements to the Director, NSA enables him to plan the effective use of his resources to conduct research with the objective of having available new cryptoprinciples and techniques to meet future specific military requirements. Similarly it is essential that detailed cryptomaterial R&D requirements be presented to the Director, NSA at an early stage in the development of new communications means. The objectives to be met in this case are:

- a. Attainment of a capability for early NSA-Military Department agreement on how best to use the combined R&D resources of NSA and the Military Departments to meet the requirements.
- b. Increased assurance of timely availability to the Services of cryptosecurity means which are compatible with their communications means.

III. SUBMISSION OF REQUIREMENTS

1. Long-range Military COMSEC objectives and cryptomaterial R&D requirements (National Crypto-Equipment Requirements, NCER) have been formulated in the U. S. COMSEC Plan as a coordinated effort among NSA and the Military Departments. These have been reviewed by the Office of the Secretary of Defense and forwarded to USCSB to form the basis for

FOR OFFICIAL USE ONLY

DRAFT

APPENDIX I

national COMSEC objectives. To provide the necessary background and understanding of military communications and weapons systems objectives as they relate to COMSEC requirements, documentation including this information will be forwarded by the Military Departments to the Director, NSA. Examples of the types of documents considered pertinent are the Army Combat Development Objectives Guide (CDOG), Navy Master Program Objective Plan (MPOP) and Air Force Applied Research Planning Documents (ARPD's). Provision of three copies of these and other pertinent documents, on an "as-revised" basis, will be considered satisfactory.

2. To insure consideration of COMSEC in the inception stages of communications developments, no requirement for separate communications means, or for communications means which are part of a "weapons" system or other electronic system, will be approved by a Military Department or the JCS (J-6) without a statement that COMSEC has been considered, and that it is or is not a requirement during the useful life of the system.
3. If consideration of COMSEC, as outlined above, results in a stated need for cryptosecurity, then the requirement will be forwarded for appropriate action, to the Director, NSA in three copies, in its earliest (OR, OSR, GOR, QMR) and subsequent (MC, DC, development plan) stages of approval by the Military Department or the J-6, as appropriate. This is not intended to preclude any informal discussions between Service and NSA personnel at any stage of requirement generation. In describing a cryptosecurity requirement, the following information will be provided at the earliest practicable time in addition to explanatory information

FOR OFFICIAL USE ONLY

DRAFT

APPENDIX I

concerning the requirement for the communications means:

- a. The approximate time period, after transmission, during which information passed over the system will require protection against enemy exploitation.
 - b. The nature and type of information to be processed (including any unusual characteristics) and, if known, the expected traffic load per cryptonet per cryptoperiod.
 - c. The proposed structure of the communications complex, including signal types, intercommunication capability (netting requirements), switching methods and operational procedures.
 - d. Any limitations of size, weight, cost or availability which, if exceeded, would absolutely preclude the use of cryptosecurity with the proposed communications means.
4. If consideration of COMSEC, as outlined above, results in a statement that cryptosecurity is not required, then the operational requirement for the communications means (systems or sub-systems) will be forwarded, for information, to the Director, NSA in its finally approved form.

IV. REVIEW OF REQUIREMENTS

1. Review of NCER's must be a continuing process in each Service. It is essential that a Joint periodic review of these requirements be assured.
2. Beginning in Fiscal Year 1961 and annually thereafter, the Director, NSA will initiate a review of the NCER's. This will be accomplished via the COMSEC Research and Engineering Committee primarily by means of an Ad Hoc subcommittee, and will include representation by the Joint Staff.

Subsequent to agreement by GREC, the amended or revised requirements will

FOR OFFICIAL USE ONLY

DRAFT

APPENDIX I

be forwarded by the Director, NSA to each Military Department and to the Joint Staff for official approval. Upon receipt of the officially approved requirements, the Director, NSA will forward these to OSD and USCSB for information.

3. Detailed military cryptomaterial R&D requirements will be reviewed annually by the COMSEC R&E Committee to determine if changes have occurred. If it is determined that changes have occurred, the Director, NSA will then take the necessary formal action to determine the extent of the change and the subsequent technical action required.

V. IMPLEMENTATION

Each Service will establish a procedure for inclusion of COMSEC considerations to coincide with the procedure now used for formulating requirements for means of communications. A copy of each document implementing this procedure will be forwarded to the Director, NSA.

VI. JOINT INTEREST

1. Consideration of Joint interest in the long range cryptomaterial R&D requirements is assured in the procedure outlined in par. IV 2. above.
2. It is essential that an indication of Joint interest in cryptomaterial R&D requirements be available as soon as practicable. Therefore, after an affirmative requirement of a Military Department is made known per III above, the Director, NSA will use the COMSEC R&E Committee to obtain an unofficial indication of Joint interest. This will be done with the full realization that subsequent official action by JCS could change this initial informal information. When appropriate the Director, NSA will

FOR OFFICIAL USE ONLY

DRAFT

APPENDIX I

correspond officially with the JCS, as provided by reference (a),
to ascertain the extent of Joint interest.

FOR OFFICIAL USE ONLY

DRAFTAPPENDIX IICOMSEC R&D PROGRAM FORMULATION AND BUDGET ESTIMATE PRESENTATION

I. RESPONSIBILITIES

1. By reference (a), the Director, NSA is required to formulate an integrated R&D program to ensure the continuing security of military telecommunications. By reference (b), the Director, NSA must submit to the Secretary of Defense a consolidated DOD COMSEC RDT&E budget together with his recommendations pertaining thereto. The Military Departments on the other hand are responsible for the preparation and justification of their proposed COMSEC R&D budgets, and for appropriate coordination of their COMSEC R&D programs with the Director, NSA.
2. While the Director, NSA is required to advise the Secretary of Defense concerning all phases of COMSEC R&D as these appear in the programs of the Military Departments, his primary responsibility will lie in the cryptosecurity R&D effort as delineated in reference (a).

II. COORDINATION

1. A semi-annual technical assessment of the COMSEC R/D programs of NSA and the Military Departments will be submitted by the Director, NSA to the Director, Defense Research and Engineering. Primary emphasis in these assessments will be placed on current programs; however, future planning will be given consideration. In addition, to the semi-annual assessments, a consolidated COMSEC R/D program and budget estimate, with appropriate recommendations, will be submitted annually by the Director, NSA to the Director, Defense Research & Engineering. Primary emphasis on this will

FOR OFFICIAL USE ONLY.

DRAFT

APPENDIX II

be on the program for the fiscal year following the one in which the submission was accomplished.

2. To permit coordination of the COMSEC R&D programs and an understanding of their content, a proposed schedule of coordination is outlined below.

Specific times are referred to a current fiscal year C.

- a. April, Fiscal year C - NSA holds informal conferences with Military Department representatives to discuss progress on C-year programs and plans for (C/1) year programs. Primary emphasis will be placed on those programs which did not receive recent or sufficient discussion in the COMSEC R&E Committee.
- b. May, fiscal year C - NSA prepares assessment of the Defense-wide COMSEC R&D programs.
- c. June, fiscal year C - NSA forwards assessment of b. to DDR&E.
- d. August, fiscal year (C/1) - Military Departments submit approved programs and budget estimates for fiscal year (C/2) to NSA.
- e. September, fiscal year (C/1) - NSA submits consolidated COMSEC R&D program/budget estimate, with appropriate recommendations, to DDR&E.
- f. October, fiscal year (C/1) - NSA holds informal conferences with representatives of Military Departments to discuss progress and plans on (C/1) year programs and proposals on (C/2) year programs. Emphasis is placed on programs which did not receive recent or sufficient discussion in the COMSEC R&E Committee.
- g. November, fiscal year (C/1) - NSA prepares assessment of the Defense-wide COMSEC R&D programs.

FOR OFFICIAL USE ONLY.

DRAFT

APPENDIX II

- h. December, fiscal year (C/1) - NSA forwards assessment of g. to DDR&E.
3. In the field of cryptosecurity R&D, a program approved in the formulation stage is not necessarily one approved for implementation. A separate procedure is delineated in APPENDIX III for the pursuit of such programs.

FOR OFFICIAL USE ONLY

CONFIDENTIALCONFIDENTIALDRAFTAPPENDIX IIIIMPLEMENTATION, REVIEW AND CONTROL OF
COMSEC R&D PROGRAM

I. POLICY

1. One of the objectives of reference (a) is to improve the utilization of cryptologic research and development resources. In this connection the National Security Agency has been assigned the responsibility, under the supervision of DDR&E, for formulating an integrated cryptosecurity R&D program and coordinating that portion of the cryptosecurity R&D conducted by the Military Departments. It is imperative, however, that participation by the various departments be established only under conditions which are consistent with the basic aim of centralized responsibility, viz., economical and effective use of resources.
2. A number of different factors must be considered in arriving at a determination as to where a specific cryptographic R&D project should be conducted and these factors will vary from one project to another. Therefore, in order to assure the best utilization of available resources in every case, this determination should be made on an individual basis. In general, however, there are three circumstances in which decentralized development will usually be desirable.
 - a. In those cases where communications systems with integrated COMSEC features are required, there are practical advantages to be gained by having the developer of the basic communications systems design and engineer such features into the overall system.

CONFIDENTIAL

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DRAFT

APPENDIX III

- b. In those cases where an individual department or agency has a unique requirement for specialized cryptographic equipment, such a requirement may often be satisfied efficiently and economically if the development is undertaken by that organization, provided that the development is based on approved cryptoprinciples. (Centralized R/D facilities may be more effectively utilized for work on new principles and on meeting requirements of broader interest and application.)
 - c. In those cases where secure communication systems must include components which are not basically cryptographic in nature, but which are necessary to facilitate the cryptographic process, the development of these components can often be most efficiently done by the developer of the communications system.
 3. On the other hand, there is no authority and there appears to be no advantage to decentralizing the responsibility for determining the security of cryptoprinciples and the security provided by specific applications thereof. The assignment of responsibility and the guidelines for the conduct of crypto-equipment development herein outlined are based on these general concepts.

II. NON-CRYPTO COMSEC R&D

1. Non-Crypto COMSEC R&D is exemplified as follows:
 - a. Physical Security - Destruction or cryptozeroizing devices; enclosures, such as safes, primarily or specifically for protection of cryptomaterial.

~~CONFIDENTIAL~~

CONFIDENTIAL~~CONFIDENTIAL~~DRAFTAPPENDIX III

- b. ~~Transmission Security~~ - Secure cable; spurious radiation detection and elimination; ~~communications means~~, the primary purpose of which is to minimize or avoid interception.
- c. ~~Crypto-ancillary equipment~~.
2. When development planning has begun, subsequent to requirement approval within the Military Department, the National Security Agency will be included as an Interested Agency in all such documentation. Three copies of final documents in this connection will be forwarded to the Director, NSA. When such R&D is part of a larger program, every attempt will be made to identify the COMSEC aspects of the program. Documentation forwarded to NSA will identify, as far as possible, the relationship to requirements documentation, estimated costs and whether this is part of a previously submitted program.
3. In some instances, a low detectability, anti-jamming, or "anti-control" characteristic is required in a communications system. In order to obtain this characteristic, techniques are utilized which, in order to be successful, depend on a resistance to analytical reconstruction. Where such techniques, namely sequential coding techniques, are utilized, it will be considered in the national interest for the developing agency to consult NSA, in the early development stages, to obtain assistance in determining the susceptibility of the system to analysis.
4. Initial program documents will be brought up for discussion at an appropriate meeting of the COMSEC R&E Committee to permit the members to be aware of current activities.

CONFIDENTIAL

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DRAFT

APPENDIX III

5. In the conduct of such R&D by the Military Departments the Director, NSA will be provided with the following documentation, in three copies:
 - a. Contractor progress and special reports as required by the contract.
 - b. Annual project and/or change-in-status report required by current Military Department R&D procedures.
 - c. Special test reports produced by the Service organization directly responsible for this R&D.
6. The National Security Agency, in its conduct of such R&D will make reports available to the Services as is now provided for or as may be agreed in the COMSEC R&D Committee.

III. CRYPTOSECURITY R&D

1. When development planning has begun, subsequent to requirement approval within the Military Department, the National Security Agency will be included as a coordinating Agency. Cryptosecurity R&D will be coordinated with the Director, NSA prior to implementation. Such coordination may occur concurrently with development planning within the Military Department.
2. If a Military Department desires NSA cooperation in the preliminary planning phase of a communications system development, such a request should be made to the Director, NSA outlining the type of NSA participation required. That Agency will provide any assistance within its capabilities.
3. When a Military Department proposes to conduct cryptosecurity R&D, the

~~CONFIDENTIAL~~

CONFIDENTIAL~~CONFIDENTIAL~~DRAFTAPPENDIX III

following procedures will be followed:

- a. A formal request will be made to the Director, NSA to provide a cryptoprinciple (or, alternatively, to approve a proposed cryptoprinciple) for use in conjunction with the planned communications system. A separate request for provision or approval of a cryptoprinciple will be required for each separate equipment or system development and/or application envisioned.
 - b. To permit proper evaluation, each request must be accompanied by three copies of a description and development plan for the proposed secure communications system. Preferably this information should be supplied on a Form DD-613 completed in accordance with the latest issue of the DOD R/D Project Card Manual. In preparing this document the relationship of the proposed R&D to previously expressed requirements, to earlier program documents and to the program of which it is a part should be identified to the greatest practicable extent. In addition to the development plan, and if not included as part of this plan, specific information relative to the security requirement should be provided as it becomes available and should include those items listed in Appendix I, Section III, pars. 2 and 3.
4. Upon receipt of the above information, the Director, NSA will make a preliminary evaluation of the cryptographic aspects involved and indicate his concurrence in the development proposal or provide alternative

CONFIDENTIAL

~~CONFIDENTIAL~~CONFIDENTIALDRAFTAPPENDIX III

recommendations to the interested Military Department. In so doing, he will take the following factors into consideration:

- a. Whether the cryptoprinciple involved is to be integrated into a communications equipment or system already under development cognizance of that Military Department.
 - b. The extent of possible or expressed Joint interest and method for insuring full coordination.
 - c. Related developments.
 - d. State of the cryptographic art.
5. If it is mutually agreed that the cryptodevelopment proposed for conduct by a Military Department is in the best interests of national security, then the Director, NSA will:
- a. Provide a cryptoprinciple to the developing agency in one of the following forms, as appropriate:
 - (1) Logical design and block diagram of an appropriate crypto-unit.
 - (2) Schematic drawings of the crypto-unit.
 - (3) Operating model of the crypto-unit in early developmental form.
 - b. Alternatively, evaluate any proposed cryptoprinciple submitted to him. If found satisfactory for its intended application, he will approve its continued development. If found unsatisfactory, he will so advise and endeavor to provide a suitable substitute.
6. At the time of provision of a cryptoprinciple or tentative approval of a proposed cryptoprinciple, the Director, NSA, will specify minimum

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CONFIDENTIAL

DRAFT

APPENDIX III

physical security requirements and any other special requirements applicable to the particular project. In the usual case, he will assign an NSA representative to the project who will thereafter conduct all necessary working-level liaison and technical coordination with the developing agency.

7. Proposals by a Military Department for cryptosecurity R&D will be presented to the COMSEC R&E Committee. An informal expression of opinion regarding the extent of interest of other Services can thus be obtained and the groundwork laid for formal determination of Joint interest.
8. In the subsequent conduct of this R&D by a Military Department the responsibilities assumed by that Military Department for the various aspects of the program are delineated below:
 - a. Coordination with NSA of specifications for the crypto-unit of a hardware development.
 - b. Coordination with NSA of Security Requirements Check List, DD Form 254, prior to bid solicitation in contractual proceedings.
 - c. Continued technical liaison at project engineer level.
 - d. Meeting Joint requirements to the mutual satisfaction of the Military Department conducting the development, other interested Services and NSA.
 - e. Provision of reports, in three copies as follows:
 - (1) Bi-monthly activities report from the developing

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~~~CONFIDENTIAL~~DRAFTAPPENDIX III

Agency directly responsible for the project.

- (2) Contractor progress and special reports as required by the contract, within 30 days after receipt by the Contracting Agency.
 - (3) Change-in-status, quarterly management and annual project report required by current Military Department R/D procedures.
 - (4) Special test reports produced by the developing agency.
- f. Notification to NSA of any logic design changes required of the crypto-unit or design changes of the system which will affect the internal design of the crypto-unit.
 - g. Performance of tests required by NSA for security evaluation of the cryptosystem.
 - h. Preparation of maintenance and operating instructions based on mutual agreement between NSA and the Military Department.
 - i. Preparation of all drawings and furnishing NSA with at least one complete set.
 - j. Training of all personnel of the Military Department conducting the development and cadre personnel of interested organizations. Training of personnel, beyond cadre, of other interested organizations will be based on mutual agreement with the Military Department conducting the development.
 - k. Procurement of all models of equipment for test including those required by NSA and other interested Services and Agencies.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~~~CONFIDENTIAL~~DRAFTAPPENDIX III

Suitable financial arrangements will be made between the Military Department accomplishing the procurement and other interested Services and Agencies.

9. The responsibilities of NSA in connection with Cryptosecurity R&D conducted by the Military Departments are as follows:
- a. Responsibility for COMSEC aspects throughout the program.
 - b. Technical assistance within the limits of available manpower.
 - c. Provision of final evaluation of paper design of crypto-principle no more than six months after initiation of the project.
 - d. Provision of specifications for and/or performance of tests required in connection with COMSEC evaluation of the hardware.
 - e. Provision of nomenclature.
 - f. Timely preparation of maintenance and operating instructions by NSA-Military Department agreement and timely provision of cryptokeying materials.
 - g. Maintenance of an office of record for drawings, specifications and design changes for all crypto-equipment.
10. In the event the Director, NSA is of the opinion that the cryptosecurity R&D proposed for conduct by a Military Department is considered to be unnecessary or undesirable, then the Director, NSA will make his opinion known to the originating Military Department with a copy of the correspondence forwarded to the Director, Defense Research and Engineering. The Military Department in order to initiate the program, will be required

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~~~CONFIDENTIAL~~DRAFTAPPENDIX III

to appeal the case to the Director, Defense Research and Engineering, with a copy of the correspondence forwarded to the Director, NSA. The Director, Defense Research and Engineering will make his decision known to both the Director, NSA and the originating Military Department.

IV. IMPLEMENTATION

The procedures of this Appendix will be implemented by each Military Department in the most practicable manner to include appropriate action levels. A copy of each implementing document will be forwarded to the Director, NSA.

~~CONFIDENTIAL~~