NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

NSA [redacted]-80
9 December 1980

~~TOP SECRET~~

MEMORANDUM FOR THE SPECIAL ASSISTANT, OFFICE OF THE SECRETARY OF DEFENSE

SUBJECT: Transition Coordination

1. Please refer to your memorandum of November 11, 1980, subject as above.

2. I am pleased to provide the enclosed material for use by the transition team. Mr. Silverstein visited the National Security Agency recently and, as a result of those discussions, our input is focusing on specific subjects in which he has expressed an interest. General introductory information and factual data concerning this Agency is also included.

3. I am prepared to follow-up as deemed necessary on these and other subjects that may arise over the next several weeks.

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

B. R. INMAN
Vice Admiral, U. S. Navy
Director, NSA/Chief, CSS

Encls:
a/s

APPENDED DOCUMENTS CONTAIN
[redacted]

~~TOP SECRET~~

TRANSITION BRIEFING BOOK

I. Introductory Section

- Mission and Authorities
- The SIGINT Process (Overview)
  - SIGINT Requirements System (Chart)
- The COMSEC Process (Overview)
- National Intelligence Community Structure (Chart)

II. Organization

- Chart with Key Personnel Named
- Civilian Grade Distribution
- FY 1981 Manpower Allocations

III. Program and Budget

- Overview
- FY 1981 Budget (Breakdown Chart)
- CCP Budget by Target - FY 1981 (Chart)

IV. The NSA/CSS Planning Process

V. SIGINT Highlights

- Major Accomplishments

VI. Communications Security

- Description and Objectives
- The National Communications Security Committee
- [redacted]

VII. Legislative Summary

- Initiatives
  - 96th Congress
    - SCES
  - 97th Congress
    - Cryptologic Equipment Fund
    - Cryptologic Grant Program
    - Protection from Liability for Psychologists
    - Transportation of the Remains of Deceased Employees, Dependents and Household Goods
  - Charter Legislation

VIII. Issues

A. Management

1. E.O. 12036
   Relative to the Budget Process
   Relative to Requirements and Tasking
   Relative to Restrictions
2. [redacted]
3. [redacted]
4. NSA Relationship with DASD(I)

B. Fiscal and Budget

1. [redacted]
2. Modernization Objectives
3. [redacted]
4. Ten-year Facilities Plan

C. Other

1. Basing
   NSA Acquisition of [redacted]
2. Administrative Subjects
   Civilian Hiring Requirements FY 1981
   Hiring Limitations/Freeze and Impact
   FOIA
   Impact of Recent Laws and Court Decisions of Personnel and Personnel Security Matters
   Economic Consequences of Field Assignments
   Shortage of Middle-Level Military Cryptologic Technicians
   Excessive Delays in Completion of Special Background Investigations (SBI's) conducted for NSA by the Defense Investigative Service (DIS)
3. Apex
4. Public Cryptography
5. [redacted] Intelligence System
6. [redacted]
7. Processing of Data from [redacted]
8. [redacted]
9. Ratio of Contract Work Supporting Hardware Maintenance/ Engineering and Software Maintenance/Development

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

MISSION

(U) The National Security Agency was established by Presidential Directive in 1952 as a separate organized agency within the Department of Defense. The Agency was assigned two primary missions - a Communications Security mission and a Communications Intelligence mission. The Director, National Security Agency reports to the Secretary of Defense. An Electronic Intelligence mission was added in 1958. The Central Security Service was established by the Secretary of Defense in 1971 and was placed under the Director, NSA.

(U) As provided in Executive Order 12036 the Secretary of Defense conducts, as the executive agent of the United States Government, signals intelligence and communications security activities. The Secretary of Defense discharges these executive agent responsibilities through the Director, National Security Agency.

(U) The responsibilities of the Director, National Security Agency/ Chief, Central Security Service include:

- the establishment and operation of an effective, unified organization for signals intelligence activities;

- collection of signals intelligence information for national foreign intelligence purposes in accordance with tasking by the National Intelligence Tasking Center;

- processing of signals intelligence data for national foreign intelligence purposes consistent with standards for timeliness established by the Director of Central Intelligence;

- executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;

- conducting research and development to meet the needs of the United States for signals intelligence and communications security.

(U) The Director, National Security Agency/Chief, Central Security Service directs and manages the United States signals intelligence system, an entity that is comprised of (A) the National Security Agency (including assigned military personnel); (B) those elements of the military departments and the Central Intelligence Agency performing signals intelligence activities;

[redacted]

(U) Relevant current documents:

- National Security Council Intelligence Directive No. 6, Signals Intelligence, 17 February 1972

- National Communications Security Directive, 20 June 1979

- Presidential Directive/NSC-24, Telecommunications Protection Policy, November 16, 1977

- DoD Directive S-5100.20, The National Security Agency and the Central Security Service, 23 December 1971

- DoD Directive S-3115.7, Signals Intelligence, 25 January 1973

- DoD Directive C-5200.5, Communications Security (COMSEC) (U), 13 April 1971

- Executive Order 12036, United States Intelligence Activities, 26 January 1978

NOTE: Proposed legislation which would provide a legislative charter for NSA was introduced in the 96th Congress. It is unlikely that floor action will occur during this session.

THE SIGNALS INTELLIGENCE PROCESS - OVERVIEW

~~(S)~~ The United States SIGINT Systems (USSS) includes the National Security Agency and the SIGINT components of the military departments; the U.S. Army Intelligence and Security Command, the Naval Security Group Command, and the U.S. Air Force Electronic Security Command. [redacted]

~~(S)~~ The USSS responds to requirements expressed by the Director of Central Intelligence and collection tasking is levied upon signals intelligence field operating activities which are located [redacted] Time-sensitive requirements are received directly from the military services to support their tactical needs.

~~(S)~~ [redacted]

THE COMMUNICATIONS SECURITY PROCESS - OVERVIEW

(U) The overall goal of communications security (COMSEC) is to protect all national security and national security related communications from foreign adversary exploitation. Operations of particular concern for COMSEC are those conducted by:

a. The National Command Authority (NCA);

b. Joint Chiefs of Staff (JCS);

c. Unified and specified military commands; and

d. Individual military units, especially combat units.

COMSEC efforts are aimed at increasing the reliability and life expectancy of existing COMSEC hardware and integrating appropriate COMSEC measures into early development stages of new and advanced communications systems.

~~(C)~~ As a primary mission, executing the COMSEC responsibilities of the Secretary of Defense as the U.S. Government's Executive Agent, NSA's role includes the following principal responsibilities:

1. Prescribe or approve all cryptologic systems and techniques used to protect national security related information from exploitation or disruption;

2. Perform R&D to fulfill requirements of the departments and agencies and to advance COMSEC technology;

3. Generate and produce COMSEC material;

4. [redacted]

5. Maintain an overview of COMSEC resources;

6. Prescribe minimum COMSEC security standards; and

7. Develop and promulgate COMSEC doctrine.

NSA/CSS CIVILIAN GRADE DISTRIBUTION

(as of 1 December 1980)

GRADE LEVEL	NUMBER
Exec Level	[redacted]
GG-18	
GG-17	
GG-16	
GG-15	
GG-14	
GG-13	
GG-12	
GG-11	
GG-10	
GG- 9	
GG- 8	
GG- 7	
GG- 6	
GG- 5	
GG- 4	
GG- 3	
GG- 2	
Wage Board	
TOTAL	

AVERAGE GRADE

End FY80	10.36
End FY79	10.32
End FY78	10.42
End FY77	10.42
End FY76	10.40

*does not include contractor personnel

NSA/CSS FY1981 MANPOWER ALLOCATIONS

Organization	Civilian Auth	Civilian Asgd	Military Auth	Military Asgd	Total Auth	Total Asgd
Director and Staff	[redacted]					
IG						
GC						
ADIL						
DDA/TDNCS						
DDPR						
DDPP						
DDO						
DDR						
DDC						
DDT						
Cryptologic Career Development						
TOTAL HQ						
FIELD						
TOTAL NSA/CSS						

PROGRAMS AND BUDGET

Introduction

As of 5 December 1980 the defense appropriations measure affecting the three NSA-related programs had technically completed House-Senate conference action and was awaiting Senate floor action. House floor action will also be required should the Senate approve the conference agreement.

The following is a summary description of the three NSA-related programs and is accompanied by a summary budget chart for FY 1981, as of 24 November, as NSA is specifically affected.

The figures in the FY 1981 Budget summary do not reflect final Congressional action on appropriation requests or the impact of pay supplemental decisions.

I. Signals Intelligence

A. Consolidated Cryptologic Program

The Director, NSA is responsible for the management and operational control of the worldwide U.S. signals intelligence effort. A majority of that effort is funded in the Consolidated Cryptologic Program (CCP) for which the Director is Program Manager. Certain resource requirements [redacted] other specialized Defense activities also contribute to the SIGINT mission and are funded separately.

The FY 1981 budget supporting the total Consolidated Cryptologic Program was originally submitted at a total of [redacted] (See CCP chart for target breakdown). This budget was the final product of a process which began with a comprehensive program review conducted centrally at NSA and involving the cryptologic components of the military departments [redacted] and other concerned agencies. After approval of this program by the Secretary of Defense and [redacted] a Zero Base Budget was formulated by NSA and each department [redacted] These component budgets were then combined and ranked as a total consolidated cryptologic budget for final decision by the DCI and the President.

The NSA share of the CCP is [redacted] as of 24 November.

B. Tactical Cryptologic Program

The Tactical Cryptologic Program (TCP) consists of those resources and activities of the three Military Departments and the National Security Agency engaged in tactical signals intelligence activities in support of tactical commanders. The Tactical Cryptologic Program is a major functional program within the Intelligence Related Activities Aggregation of the Defense Budget. The TCP was established in 1979 to correct the problem of disparate requirements competing for limited available funding within the National Foreign Intelligence Program which resulted in inadequate treatment of Service tactical support needs.

The mechanism proposed by the Secretary of Defense and approved by the Executive Branch establishes the Tactical Cryptologic Program with the Director, NSA as Program Manager. The creation of this program aggregation is in consonance with Congressional direction with respect to the unitary review and control of all signals intelligence activities by the Director, NSA.

Program decisions by the Secretary of Defense form the basis for TCP budget development. The military services coordinate their individual budget development with the Director, NSA.

The FY 1981 TCP was justified at [redacted] of which [redacted] is the NSA share.

II. Communications Security Resources Program

The Director, NSA, executes the responsibilities of the Secretary of Defense as Executive Agent for the Communications Security (COMSEC) of the United States Government. That effort is funded in the Communications Security Resources Program which encompasses the budget requirements of the military departments, the National Security Agency, and the Defense Intelligence Agency.

The COMSEC budget for FY 1981 was justified by the Secretary of Defense [redacted] allocated to NSA.

FY 1981 BUDGET ($ in millions)

CCP

Military Pay

Operations and Maintenance

Procurement

RDT&E

Military Construction

TOTALS

TCP

Military Pay

Operations and Maintenance

Investment

RDT&E

TOTALS

CRP

Military Pay

Operations and Maintenance

Procurement

RDT&E

Military Construction

TOTALS

[redacted]

COMMUNICATIONS SECURITY

The COMSEC mission of NSA is a vital element of national security and the implementation of national security policy. Its scope is vast and our involvement with our customers is close and continuing. The exploding technology and the rapid expansion of information processing and transmission is correspondingly expanding the volume and type of COMSEC solutions and applications required. The challenge and responsibility is immense in view of the absolute necessity [redacted] achieve and maintain an acceptable COMSEC posture [redacted] and other national security related communications.

The fundamental role of U.S. Communications Security (COMSEC) is to deny to the enemy the ability to derive from U.S. classified and unclassified communications information detrimental to our national security and his ability to decrypt these communications. The Secretary of Defense is the Executive Agent of the Government for Communications Security. NSA is the principal arm of the Executive Agent in carrying out of the COMSEC mission.

The COMSEC mission is extremely complex and multi-faceted in scope.

1. Our users run the gamut from the President to infantry maneuver units with the entire wide range of sensitivities and applications involved. Although a Defense Agency, NSA's responsibility for providing COMSEC for national security information is Government-wide.

2. COMSEC applications range from protection of [redacted] to providing authentication for [redacted]

3. COMSEC needs must be met for a wide variety of communications-electronics categories including voice, teletype, data, telemetry, TV, facsimile, and computers/ADP.

4. The COMSEC responsibility of NSA embraces the full cycle from enemy threat analysis, vulnerability assessment, cryptologic research, development of COMSEC equipment and codes, their consolidated production for the entire Government, providing the doctrine for their secure use, life-time provision of parts and cryptologic materials, working with the users to apply them effectively and efficiently, and throughout the entire process continually assessing their security.

5. In addition to providing cryptographic protection [redacted] the communications themselves, [redacted] We must also provide protection [redacted] Finally, we must provide cryptographic techniques to protect [redacted]

[redacted]

6. To provide a cohesive basis for such a vast scope, as the principal working elements of the Government for COMSEC, NSA develops policy, objectives, and plans for review and promulgation by the National Communications Security Committee. As the COMSEC Program Manager for DoD, NSA also has the responsibility for assuring an optimal program balancing current and projected needs.

7. Added to these functions is the lead role NSA must play in assuring [redacted]

Our COMSEC must be effective against the enemy's signal intelligence (SIGINT) effort. [redacted]

In recognition of the threat to U.S. communications and in consonance with the national policy expressed in Presidential Directive/NSC-24, special emphasis is being placed on expansion of [redacted] Attached is a somewhat more detailed description of these and other NSA activities that are relevant.

Also attached are brief descriptions of the National Communication Security Committee (NCSC) [redacted] NSA role in each is identified.

ATTACHMENT 1 TO COMSEC

A. Voice. [redacted] A secure voice equipment designed [redacted] is also entering initial production. The need for aggressive secure voice action is still dominant [redacted] and continued pressure is required to assure that the Military Services and important civil government activities continue to procure the equipment at the rates dictated by the NCSC policy on secure voice. Achieving [redacted] meeting DoD fixed-plant requirements [redacted] the DoD communicators and NSA [redacted]

B. [redacted] The positive control over [redacted] has been an element of national security policy that NSA has been deeply involved in for [redacted] NSA has designed and produced [redacted] and COMSEC devices for [redacted] A major future impact is the [redacted] which will require a very heavy expenditure of NSA COMSEC talent and development resources to provide the needed security.

C. Record and Data. Providing COMSEC for record and data communications is another important effort. We are currently providing new equipments [redacted] The explosion in data and ADP communications is changing the complexion of the COMSEC problem since it is beginning to assume a significant share of the traffic volume as compared to voice communications, which heretofore was overwhelmingly predominant.

D. [redacted] From virtually the start of [redacted] NSA has been deeply involved in providing security [redacted] to prevent enemy manipulation and consequential negation of [redacted] and in providing security for [redacted] We have an enviable record of successful performance in this field. Currently, we are providing [redacted] capabilities for the [redacted]

E. Computer Security. The rapid, almost explosive use of computers and their rapidly advancing technology has provided great difficulties in achieving requisite security for processing classified information. NSA has taken the lead in developing techniques for "trusted" computer designs, cryptologics for protecting information in the systems, authentication schemes for protecting against unauthorized access and manipulation and a host of other aspects. The problem still looms large and it is growing. [redacted]

[redacted]

G. [redacted]

H. Technology. The successful fulfillment of our COMSEC mission requires us to be at the forefront of the communications-electronics technology world as well being the experts in the field of cryptology. We are currently giving [redacted] communications [redacted] security as well [redacted]

I. Secure [redacted] Taking the lead in COMSEC [redacted] is a time consuming, resource consuming activity, but one which can be [redacted] COMSEC [redacted] an active COMSEC area. [redacted] NSA has been the architect of a COMSEC approach for providing the necessary security [redacted] without serious impact [redacted] This proposal has recently been adopted as national policy and is in the active implementation planning stage.

J. Protection of Commercial/Private Sector Communications. [redacted] Presidential Directive 24 has assigned the focal point for protecting non-national security information to the National Telecommunications and Information Agency (NTIA) of the Department of Commerce. NSA and NTIA coordinate closely in view of the close relationship of our missions, with NSA continuing to provide the lead for cryptologic development and techniques.

K. COMSEC Assessment. A considerable emphasis in our current actions is the development of capabilities to assess our COMSEC posture. As systems and applications become more and more complex, it is increasingly possible for a combination of systems and use factors to impact the security provided by COMSEC equipment. To counter such conditions, it is becoming increasingly important [redacted] assess the degree of COMSEC being achieved in use. Modern quantitative analysis techniques are being utilized [redacted]

L. COMSEC Material Production. The production of codes and COMSEC equipment for the entire Federal Government [redacted] requires a great amount of talent and resources, but is one in which we have an excellent record of performance. We produce [redacted] of codes and key setting for equipments which are distributed worldwide on a priority basis by the military system. Last fiscal year, we administered contracts [redacted] equipments, ancillary units and parts. Singled out for exceptional note by OMB was the savings on the production [redacted] equipment over a three year period (78/80) [redacted] due to NSA procurement strategies. In addition, in FY 80 we [redacted] consolidating the Services' requirements for production [redacted] by rehabilitating and redistributing excess COMSEC equipment.

M. COMSEC Manpower. The key ingredient to NSA's fulfillment of its complex COMSEC mission is its well qualified and highly motivated workforce. There is no source outside of NSA for acquiring qualified COMSEC professionals, and at a time of rapidly expanding demands on the COMSEC mission it is becoming increasingly difficult to attract the manpower with the potential for becoming COMSEC professionals. This is a roblem for the immediate and longer range future that could have a significant impact if solutions are not found.

ATTACHMENT 2

NATIONAL COMMUNICATIONS SECURITY COMMITTEE

(U) The body that is now known as the National Communications Security Committee (NCSC) was established by a Presidential Directive in October 1952, at which time it was designated the United States Communications Security Board (USCSB). NSA provides the Executive Secretary to this committee.

~~(C)~~ With the approval of the National Communications Security Directive of June 1979, the USCSB was renamed the National Communications Security Committee (NCSC) with a representative of the Secretary of Defense as Chairman and composed of representatives designated by State, Treasury, the Attorney General, the Secretary of Transportation, the Secretary of Energy, the Secretaries of the Army, Navy, and Air Force, the Director of Central Intelligence, and the Director, National Security Agency. The Directive further stated that representatives of Commerce, the Joint Chiefs of Staff, General Services Administration, Federal Communications Commission, the Manager of the National Communications System, Defense Communications Agency, Defense Intelligence Agency, Defense Logistics Agency, and the Federal Emergency Management Agency may participate as observers in all aspects of the Committee's work.

~~(C)~~ The Committee was made responsible for developing for approval by the Secretary of Defense broad communications security objectives, policies and implementation procedures; providing guidance and assistance to the departments and agencies of the Federal Government in their communications security activities; conducting an annual review of the status and objectives of the communications security activities of the departments and agencies and making recommendations concerning those activities to the Secretary of Defense; providing communications security guidance to departments and agencies [redacted] and considering and discussing issues of communications security referred to it by any department or agency and making recommendations to the Secretary of Defense with respect thereto, if appropriate.

~~(C)~~ On July 10, 1979, the Executive Agent for COMSEC, the Secretary of Defense, delegated authority to the NCSC for the oversight of policy implementation in the areas of [redacted] and the access of U.S. contractors to classified Federal telecommunications or COMSEC material.

[redacted]

~~(C)~~ The NSA COMSEC organization conducts the operation of [redacted] communications security and evaluation agency [redacted] communications security material distribution and accounting [redacted] completely [redacted] functions are largely in the evaluation and [redacted] areas, and essentially [redacted] NSA COMSEC functions [redacted] functions are to arrange for the production and distribution [redacted] keying material and COMSEC publications, and to establish [redacted] procedures for adequately handling and accounting for these materials. [redacted] provide the needed authority and feedback [redacted] cryptography [redacted] properly used and protected. [redacted] provide insurance [redacted] cryptography used is adequate to protect [redacted] information.

SUMMARY OF LEGISLATIVE INITIATIVES OF THE NATIONAL SECURITY AGENCY

Legislative Proposals Currently Pending Before the 96th Congress:

Senior Cryptologic Executive Service Act of 1980 (S.2116 and H.R. 5885): This bill would provide legislative authority to the Secretary of Defense or his designee to establish a Senior Cryptologic Executive Service within the National Security Agency. The NSA was exempted from the Senior Executive Service and merit pay portions of the Civil Service Reform Act of 1978 because of NSA's unique functions and structure as well as security concerns. The bill would enable the Director, NSA, to establish the SCES within required security constraints and to establish a merit pay system appropriate to the NSA's needs. Hearings on S.2116 were held by the Senate Governmental Affairs Committee and an amended bill was reported out by the Committee with a recommendation that the Senate act favorably on the bill. The House has not held hearings on its version of the bill which has been referred to the House Permanent Select Committee on Intelligence.

New NSA Legislative Proposals for the 97th Congress:

a. NSA has four legislative proposals that have been submitted to DoD to obtain DoD and OMB clearance for submission to the 97th Congress. These are:

(1) Cryptologic Equipment Fund: This proposal is one to amend title 31, U.S.C., to add a new section to authorize the extension of the period of availability for expenditure of appropriations when used under certain conditions for the purchase of cryptologic equipment. This proposal is designed to resolve a conflict in General Accounting Office opinions concerning the conditions under which funds from other agencies become obligated for the purposes of title 31, U.S.C.

(2) Cryptologic Grant Program: This proposal permits continuation of a program providing grants for cryptologic research. The program was initiated by NSA with the approval of DoD and in accordance with Congressional guidance.

(3) Protection from Liability for Psychologists: This proposal would amend section 1089 of title 10, U.S.C., to add to the categories of those already afforded malpractice protection the categories of psychologist, psychometrician, and psychological technician. This proposal is necessary to provide the requisite protection from potential liability to assure full and complete advice needed for personnel security adjudications and proper security protection.

(4) Transportation of the Remains of Deceased Employees, Dependents and Household Goods: This proposal would amend title 10 to authorize the payment of the costs of transporting the remains of a deceased employee, the dependents of such an employee, and the household goods of that employee from a post within the United States to the place of permanent residence of such an employee.

b. NSA also intends to submit to DoD and OMB a legislative proposal to authorize establish a graduate studies program for certain critical skills personnel for which shortages currently exist.

New Intelligence Community Proposals for the 97th Congress:

NSA would support Intelligence Community Charter legislation provided it incorporated an acceptable charter for NSA to include enumeration of functional responsibilities and needed administrative authorities. In addition, the Charter legislation should include certain needed technical amendments to the Foreign Intelligence Surveillance Act of 1978.

E.O. 12036

Relative to the Budget Process

(U) Executive Order 12036, which forms the basis for the conduct of U.S. intelligence activities, has serious shortcomings and needs to be carefully reviewed.

(S) Principal among the problems inherent in this document are those associated with the intelligence budget process. Specifically, the Executive order assigns to the DCI the authority to make resource recommendations to the President for the entire National Foreign Intelligence Program (NFIP), though approximately [redacted] intelligence assets belong to DoD. Through this process the signals intelligence budget alone in the three years through FY-81 [redacted]

(S) [redacted]

(S) The budget approach has tended to concentrate on what we can do [redacted] rather than on what the real intelligence needs of the country are. The result is an intelligence structure - particularly that related to signals intelligence - [redacted]

(U) [redacted]

Relative to Requirements and Tasking

(S) Subsequent to publication of E.O. 12036, the intelligence requirements process [redacted] Under the Order, the PRC(I) was assigned the role to "establish requirements and priorities for national foreign intelligence" and to "evaluate the quality of the intelligence product." [redacted] In addition, the DCI's staff has been [redacted] in linking National Intelligence Topics (NITs) developed by the PRC(I) to the NFIB, i.e., approved requirements process as outlined in DCID 1/2. Attempts to prioritize intelligence needs and to evaluate requirements satisfaction have been made and continue to be worked on [redacted]

[redacted]

(C) [redacted]

(U) The National Intelligence Tasking Center has never really taken shape as described, and thus its impact has been of little consequence apart from the education which took place over four years of evaluation. The "collection plans" involve Community elements in much paperwork for little, if any, tangible return.

Relative to Restrictions

[redacted]

(U)The following are some of the provisions of the Order that have produced unintended or burdensome results.. Their amendment would ease compliance with the order while not diminishing protections afforded U.S. persons.

a. Section 2-202: This section includes, inter alia, a requirement that testing and training of electronic communications equipment be subject to procedures. This is an unnecessary restriction. Intelligence agency communications devices and communicators should be treated no differently than their counterparts outside the intelligence community. This restriction should be modified to apply only to electronic surveillance equipment. In

[redacted]

addition, the provision that limits the use of data acquired during testing and training to those purposes only should be modified to permit otherwise lawful retention or use if the testing or training is conducted against signals that could be lawfully intercepted for intelligence purposes. There appears to be no sound reason to deprive the government of foreign intelligence information because it was acquired during testing or training rather than during routine operations.

b. Section 2-208: A new subsection is needed that would permit the collection of information on U.S. persons abroad when their physical safety is threatened and it is impossible to obtain their consent, e.g., hostages, POW's, or refugees. No single provision in 2-208 clearly permits such collection. Subsection 2-208(i) is not sufficiently broad. It raises legal questions concerning the scope of the Department of State's consular responsibilities particularly if the U.S. persons are in a country with which the U.S. has no diplomatic relations or are on the high seas or in international airspace.

c. Section 2-203: This section only permits concealment of contracts with non-academic institutions when "necessary to maintain essential cover on proprietary arrangements." It does not permit concealment in circumstances where a particular contract or an aggregate of contracts would disclose classified capabilities or the specific targets of an intelligence agency. This section should be modified to permit concealment in such circumstances.

[redacted]

NSA MODERNIZATION OBJECTIVES

(S) NSA has been, and continues to be faced with the need to produce intelligence information from a signals environment that is characterized by greatly increasing volumes and complexity of available communications, and to do so [redacted]
We have pursued actively a program to modernize on-site equipments and techniques [redacted] The U.S. SIGINT System, however, must continue to pursue acquisition of [redacted] and processing systems with [redacted] capabilities if we are to meet the challenges of the future.

(S) To meet these challenges, the following objectives comprise our strategy for the future:

Collection and Processing Equipment: [redacted]
to maintain pace with in-being communications and conduct research aimed at handling developing and anticipated technologies.

[redacted]

NSA RELATIONSHIP WITH DASD(I)

(S) The relationship between NSA and the DASD(I) has been quite satisfactory and beneficial in those intelligence programs under the control of the Secretary of Defense. The establishment of the Tactical Cryptologic Program (TCP) beginning in Fiscal 1981 was a major accomplishment which the DASD(I) supported. The DASD(I) also played a major role in the creation of the [redacted] which is being implemented in the FY 1982 budget.

(U) The effectiveness of the DASD(I) in Programs and Budgets under the purview of the DCI has been limited. The implementation of Executive Order 12036 which vested "full and exclusive" authority in the DCI for Intelligence Programs and Budgets within the NFIP served to neutralize the DASD(I) role in the CCP. The DASD(I) has supported NSA in the NFIP arena but most such efforts have proven fruitless. The most significant contribution made by the DASD(I) in dealing with the NFIP has been in furnishing technical and management support to the Secretary for his meetings with the DCI, OMB and the President.

(U) Restoring an OSD structure that can more effectively deal with non-DoD aspects of intelligence oversight/management is urgently needed. The DIRNSA believes that the creation of an Assistant Secretary of Defense (Intelligence) (civilian) or Director of Defense Intelligence (military with Assistant Secretary status) should be a high priority goal in the incoming administration.

TEN-YEAR FACILITIES PLAN

ISSUE: To obtain the required, properly configured, permanent facilities to house the computer-based systems and analysts employed in the Signals Intelligence mission.

EXISTING SITUATION:

-- NSA Operations initially moved to Ft. Meade in 1957.

-- Now occupy 4.6 million sq ft at Ft. Meade and Friendship Airport, and environs:

-- 3.3 million SF in permanent facilities

-- .4 million SF in temporary Government buildings

-- .9 million SF in leased commercial facilities

THE PROBLEM:

[redacted]

-- We have recently undergone a comprehensive realignment to obtain the greatest efficiencies from existing facilities and to compress analyst space to a bare minimum (45 SF per person, vice DoD standard of 80 SF).

-- A 10-Year Facilities Plan validates the need for 1.3 million SF of net useable space between now and 1990:

-- 376,000 SF to accommodate program needs through FY 1985

-- 300,000 SF to decompress analyst work areas

-- 600,000 SF to replace leased commercial facilities

-- Surveyed over 100 available U.S. Government facilities, but found none suitable.

-- Temporary measures (particularly leasing) are unsatisfactory for the long-run and very expensive (now spending in excess of $8 million in annual recurring costs associated with use of leased facilities).

THE SOLUTION:

-- In the near-term, to house programmed systems additions through FY 1985 and achieve some decompression, the construction of a 960,000 SF facility (676,000 SF assignable) has been proposed in the FY 1982 budget. Several options were examined:

-- Two separate projects, in FY 1982 and FY 1985 (total cost = $141 million)

-- A two-year, sequentially funded project, FY 1982/83 (total cost = $131.3 million)

-- A single project, FY 1982 (total cost = $121.7 million)

-- Strongly urge inclusion of $121.7 million in FY 1982 budget for a single-year project.

-- Dependent on sufficient funds from Sec Def to complete planning and design phases:

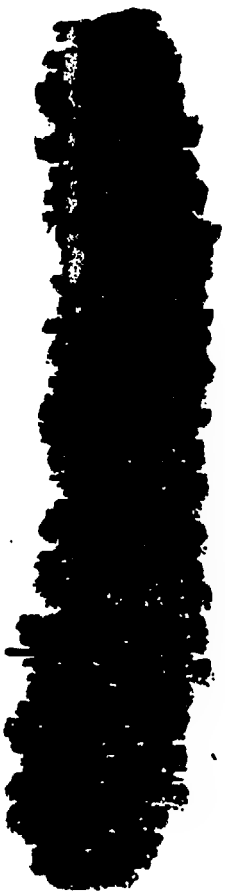
-- $3 million in FY 1981

-- $1.9 million in FY 1982

FY81 HIRING REQUIREMENTS

INFORMATION SCIENCE
SPECIAL RESEARCH
LINGUIST
CRYPTANALYSIS
TRAFFIC ANALYSIS
SIGNALS ANALYSIS
SIGNALS COLLECTION
SIGNALS PROTECTION
MATHEMATICS
ENGINEERING
PHYSICAL SCIENCE
COMPUTER SYSTEMS
TELECOMMUNICATIONS
LEGAL
SYSTEMS MANAGEMENT
SECURITY
RESOURCES MANAGEMENT
INDUSTRIAL PRODUCTION
LOGISTICS
ADMINISTRATION & SUPPORT
CRYPTOLOGIC OPERATIONS OFFICER
SYSTEMS SCIENTIST

TOTAL



HIRING LIMITATIONS/FREEZE AND IMPACT

1. (U) There is grave concern that the limitation on civilian hiring will soon seriously jeopardize our ability to fulfill critical mission requirements if action is not taken to relieve these constraints. The current limitation on civilian hiring permits the appointment of only one person for every two vacancies which occur after 29 February 1980. The limitation not only restricts the filling of vacancies occurring this year from our already eroded manpower strength but also precludes the acquisition of needed personnel for important initiatives which have already been approved by Congress. These initiatives include programs of major concern to national decision makers. We also had additional billets authorized which would permit us to carry out Executive Branch and Congressional directions for improving the management of tactical cryptologic efforts. The hiring limitation negates our ability to move ahead on these programs and seriously impairs our ability to staff other programs in areas critical to the security of U.S. communications and the production of signals intelligence.

2. ~~(S)~~ The potential impact of a total hiring freeze on NSA operations is incalculable. Assuming a total hiring freeze, we estimate that more than [redacted] authorized civilian positions would be vacant by the end of FY81. This problem is further compounded by the exceedingly long lead times required to process, clear, and appoint civilian employees to this Agency; particularly during a time when competition for critical skills places the federal government at a serious disadvantage.

3. ~~(S)~~ Without adequate staffing, particularly of positions requiring people with critical skills, it is difficult to maintain existing operating systems, much less provide for the development of new systems and software needed to support our [redacted] While we are continuing to upgrade our [redacted] that effort will require additional engineers, analysts, data systems specialists, cryptomathematicians, signals processors and support technicians.

4. ~~(S)~~ The acquisition of [redacted] trained and competent, is a major need for NSA. Workloads and diverse priorities resulting from [redacted] combine to create an ever increasing shortfall between essential [redacted] processing requirements and the available, trained [redacted] workforce. Despite the fact that the Agency is the largest employer of [redacted] in the Intelligence Community, a significant increase in authorized manning will be necessary to effectively respond to customer requirements.

5. (U) The following chart depicts the numbers and skill distribution of our hiring requirements for FY 1981 as represented by authorized vacancies and projected losses through attrition. The shortfall in the above described critical skills is readily apparent.

FREEDOM OF INFORMATION ACT

The primary problem created for the National Security Agency (NSA) by the Freedom of Information Act as amended, (FOIA) is the danger of disclosure of information and of sources and methods that are uniquely fragile and sensitive. Experience indicates that this may occur through partial or full disclosures ordered by a court, through inadvertant disclosures, either by mistake, by over-zealous administration, by exigencies of litigation, or by court review. To a lesser degree, inappropriate disclosure may also occur through violation of traditional need-to-know principles during the search and review process, or through judicial failures to safeguard information presented to the court. This is in addition to the cost of processing FOIA requests, searching necessary records, and participating in litigation.

NSA possesses some useful protection in the form of statutes requiring protection of cryptologic information, which have been identified by the Congress and interpreted by some courts as constituting exemption to the FOIA. Such an interpretation has not been made by all courts, however, and the exemption is under continuous and systematic attack by groups seeking access to NSA's records. In addition, this protection has been eroded by judicial action.

The courts are currently considering a number of FOIA cases involving NSA information in which the result could be to further erode existing protection of sensitive cryptologic information through the following actions:

a. applying a full Vaughan v. Rosen indexing requirements to cryptologic records;

b. ignoring b.(3) exemption standards and accompanying legislative history (permitting reliance on affidavits vice de novo review and examination of classified records) and substituting b.(1) exemption standards (requiring de novo review and examination of records);

c. attempting to limit the b.(3) exemption to classified information only, although section 6 of the National Security Agency Act clearly extends statutory protection beyond classified information;

d. attempting to impose administratively mandated tests such as those contained in various sections of Executive Order 12065, National Security Information, especially section 3-303 dealing with the so-called public interest balancing test.

Legislative action is required to reinforce and ensure continuation of existing protection. A broad exemption from the Act for intelligence information and records would be the most effective way to accomplish this goal. In addition, it would be useful to clarify guidance to the courts as to Congressional intent to make the b.(3) exemption broader and clearer, and less subject to judicial interpretation and nulification, and to render cryptologic records less subject to judicial administrative requirements such as indexing. While a broader, separate amendment to FOIA might be the most effective way of dealing with these issues, they can also be affected through a series of narrow technical amendments to the existing Act.

Previous Executive Orders relating to classification have also had an impact on the ability to protect sensitive information under FOIA, because of the impact of the Order on determining whether particular information is properly classified and therefore is exempted from disclosure. Administrative action is required to amend the existing Executive Order 12065 to more adequately protect cryptologic information. This could be accomplished by deleting or amending provisions contained in sections 1-6, 3-3 and 3-505, and by adding one or more new sections to the Order, to restore provisions protecting cryptologic information that were contained in previous executive orders on classification (e.g., sections 5.(B)(2) and 9 of E.O. 11652). It would also be useful to restore, at least for cryptologic (and other intelligence) records, the concept that certain, individually unclassified information may reveal sensitive information in the aggregate, and thus should be classified. There should also be a review of the concepts of segregability and portion-marking.

Finally, recognizing both the personnel and security costs of administering the FOIA program in intelligence agencies, an effort should be made to limit the need to search for and review records that prima-facie will be exempted, indexing, the requirement to segregate out and release information, and the need for judicial review and to substitute administrative certification.

IMPACT OF RECENT LAWS AND COURT DECISIONS ON PERSONNEL AND PERSONNEL SECURITY MATTERS

In order to make effective decisions regarding employment and retention of personnel in sensitive positions requiring access to classified cryptologic information, it is essential that there be available for consideration all pertinent information, both positive and negative, concerning individual applicants, employees or assignees. Timely and complete access to such information has been inhibited to a limited extent by several recent laws including the Privacy Act of 1974, and the Right to Financial Privacy Act of 1978. Presumably, the recently enacted Federal Privacy of Medical Information Act of 1980 will have a similar effect. Access to certain criminal justice records has been limited also by overly strict implementing, by the states of the LEAA guidelines on disclosure of such information. These laws tend to inhibit access to information because (1) individuals fear disclosure of the information they provide, (2) collectors of information fear sanctions for inappropriate collection and retention, and (3) collectors of information fear sanctions for inappropriate dissemination. In addition, the laws inhibit retention and use of such information because they impose sanctions on inappropriate retention and use of information in certain circumstances. It may be possible to remedy some aspects of the problem by revising the existing complicated implementing regulations rather than attempting to change the laws. It would also be useful to modify the Privacy Act public disclosure requirement concerning systems of records as they pertain to persons associated with an intelligence agency to limit the requirement for publication to disclosure to persons within the agency only. This would limit the amount of exposure of sensitive information concerning agency operations without affecting the underlying goal of allowing individuals access to information concerning them.

The most immediate and difficult problem concerning decisions on employment, assignment and retention of personnel requiring access to sensitive cryptologic information is presented by the court decision in the recent case of Jane Doe vs. U.S. Civil Service Commission, the settlement of that case by the OPM, and subsequent action by OPM to promulgate regulations based on that decision. This case and its precipitous settlement by OPM before appeal, presents the serious possibility of personal liability to individual government officials for disseminating or using derogatory information acquired during background investigations. Because of such possible liability, there has arisen the likelihood that employment or access will be granted without the benefit of full, complete background information on an individual. Because of the decision and settlement of Doe, it has been necessary to adopt stringent internal procedures limiting dissemination of information in order to protect officials involved in such matters from possible personal liability. In settling Doe, and subsequently issuing draft implementing regulations, OPM has failed to adequately distinguish between regular Government employment and employment involving access to sensitive intelligence and cryptologic information. In the more sensitive positions, consideration of all background information, regardless of the source or content, is essential to assure faulty security determinations are not made. Although there is has been an effort by the intelligence community to counter the OPM initiative, more effective action is required to avoid establishment of procedures that will further undercut personnel security. Administrative action may not be adequate since the case is grounded on a constitutional tort theory, and it may be necessary to seek legislative relief through some form of protection for officials in intelligence agencies from personal liability.

ECONOMIC CONSEQUENCES OF FIELD ASSIGNMENTS

1. The high cost of living worldwide is causing considerable hardship to NSA's Field employees, particularly those at junior grade levels. Moreover, the knowledge of these hardships has permeated the Headquarters workforce to the extent that it is becoming increasingly difficult to attract qualified employees for these vital positions.

2. Additionally, today's real estate situation adds a further complication in that many people will not accept a Field position if it means that it will cause them to become "long distance landlords." Yet, if they sell their present home, they know that the same favorable interest rate they are paying on their mortgage today, will be considerably accelerated when they return from their Field assignment.

3. Currently, there [redacted] positions scheduled to become vacant in calendar year 1981, for which no interest has been expressed from within the workforce. Many of these positions involve highly technical skills that are mission-essential (engineers, data systems analysts, etc.). If the Agency is to continue to successfully man Field positions, it is believed that more favorable entitlements and higher cost-of-living allowance will have to be provided.

SHORTAGE OF MIDDLE-LEVEL MILITARY CRYPTOLOGIC TECHNICIANS

1. As is the case throughout the military services, the impact of the declining number of middle-level non-commissioned officers and petty officers within the services has become apparent within this Agency. Within the U.S. SIGINT system, this shortage is of concern as it may reduce the effectiveness of the system in fulfilling its mission. A recent comparison of the manning levels for military enlisted personnel with the requirements by grade levels within this Agency's operational requirements shows a shortage of [redacted] personnel in grades E5 through E7. The greatest deficiency is at grade E5. The problem is further exacerbated by the fact that a sizable portion of those assigned are recent technical school graduates without field experience. This situation generates three problems: (1) Many technical military positions are currently unfilled or are manned by less qualified Junior enlisted personnel; (2) On-board, experienced, technical personnel are required to spend more time in training less experienced Junior personnel; and (3) An increasing number of Agency positions must be filled with civilians, when available, because of the non-availability of experienced enlisted personnel.

2. NSA would support any DoD initiatives to provide incentives to attract and retain these military enlisted personnel.

EXCESSSIVE DELAYS IN COMPLETION OF SPECIAL BACKGROUND INVESTIGATIONS (SBIs) CONDUCTED FOR NSA BY THE DEFENSE INVESTIGATIVE SERVICE (DIS)

1. DIS has conducted SBIs on most of the Agency's civilian job applicants and Agency contractor employees since 1972. In FY 80, we initiated approximately [redacted] DIS. As of October 1980, average case completion time by DIS was 156 days, up from 90 days less than two years ago, and far in excess of DIS's target for SBIs: 65 day completion time. DIS and OSD recognize that there is a serious problem for all DoD customers of DIS.

2. NSA has a number of serious (or potentially serious) problems because of the excessive completion times:

a. Unable to attract competitive skill persons (electronic engineers, computer specialists, for example).

b. Unable to quickly put to work persons urgently needed to accomplish NSA mission (linguists, for example).

c. Unable to fulfill terms of critical contracts, i.e., cannot grant clearance access to contractor personnel. The mission suffers and lawsuits are possible (and have happened in the past).

3. Public Law 88-290 and DoD Directive 5210.45 require that individuals have had completed SBI prior to employment, assignment or detail to NSA.

4. NSA supports immediate manpower increase for DIS.

APEX ISSUES

~~(C)~~ As we move closer to APEX, a number of problems have become apparent. The original objectives of the program and the basic, essential concern for security are becoming lost. They are being obscured by the large number of detailed, sometimes conflicting, implementation instructions contained in interpretations of the provisions of the NFIB Final Report and subsequent APEX manuals, reactions to procedural proposals, and ad hoc statements of guidance by the APEX Steering Group and its various Sub-committees. We believe it is essential to reevaluate whether APEX, as we now understand it, is worthwhile or cost-effective. In view of the large resource costs and security risks associated with the implementation of APEX as we currently perceive it, several major issues must be clarified. These issues are:

1. ~~(C)~~ Information Security

Rather than providing additional security as intended, APEX security procedures appear to increase the opportunity for signals intelligence loss, espionage, and security compromise.

- The general attribution to COMINT tells the opposition where the information came from, and thus where to look to block future exploitation of those communications.

- [redacted]

- The potential of a major security compromise both of the new system and the existing system is inherent in the concurrent use of both existing and new procedures during the phasing process. Additionally, under APEX a hard copy document gets new controls and markings while the same information as that contained in the document is marked according to existing control systems when transmitted electrically.

2. ~~(C)~~ Expense

While APEX gives the appearance of administrative simplicity, it is in fact far more complex and costly in its application than our current COMINT handling system. Conservatively, in additional [redacted] billets plus the people costs associated therewith together with [redacted] for communications, computer and other modifications are

required to implement APEX in the U.S. SIGINT System based upon our understanding of the procedural requirements. Since the DCI has directed that these manpower and dollar costs be absorbed by the Program Managers, APEX implementation will be at the expense of existing SIGINT production and reporting.

3. ~~(C)~~ Intelligence Involvement in the "Electronic Age"

The emphasis of any security control system must be placed upon protection of information, regardless of medium. APEX imposes special controls only on that information which is hard copy (printed form) and handled via courier. However, the trend in transmitting intelligence information is away from hard copy use and toward an electronic, paperless environment. For example, less than [redacted]

4. ~~(C)~~ Legal Implications

In formulating APEX, the APEX staff has repeatedly dismissed serious legal problems raised by the proposed APEX procedures. Especially serious is the dilution through APEX of existing statutory requirements and protections related to cryptologic information and access thereto. This unique set of protection was enacted by Congress after long study of existing problems and needs. In addition, the APEX nondisclosure agreement raises the potential for new complex litigation, as well as serious administrative/legal problems with implementation, particularly with respect to current employees, assignees and contractors.

5. ~~(C)~~ SIGINT and the APEX Model

a. APEX arbitrarily divides the SIGINT categories of COMINT, ELINT and TELINT into two separate product compartments. It mixes ELINT and TELINT with non-SIGINT information in the "TECHNICAL" product compartment. Operational information pertaining to all three categories is retained in the COMINT Operational Compartment. This unnatural fragmentation endangers sensitive information.

b. APEX separates intelligence information from production information and presupposes the existence of a SIGINT Operational Compartment to hold source/method data apart from SIGINT intelligence information. This concept appears to engender significant administrative burden without commensurate benefit. [redacted] Rather than pursue uniformity for the sake of uniformity, we need to reconsider what, if any, change is required in the present handling of SIGINT.

PUBLIC CRYPTOGRAPHY

Interest in cryptology in the public sector, paritcularly from the academic research community, is a subject of continuing concern to NSA. Efforts made in establishing a dialogue with both the government and the non-governmental community to stimulate useful research on cryptography and a better understanding with academe of the security implications of the public study of cryptography have been productive. Toward that end, NSA has participated in forums with the American Council on Education (ACE), the National Science Foundation (NSF), and individual universities and scholars to address issues of academic freedom and national security. The ACE Public Cryptography Study Group is studying this subject under an NSF grant and will soon publish a report which will recognize the Government's concerns about the national security impact of open research, commercial development, publication, and discussion of cryptology in the public sector. The ACE report will encourage voluntary cooperation with NSA in terms of providing us prepublication review of reports and articles dealing with cryptology. With the cooperation of NSF, we have recently established a complementary grant program to fund relevant cryptologic research, most of which will be unclassified. This program will serve as a forum in which the academic community can exchange views on cryptologic research. Within DoD, initiatives toward coordination of cryptologic research funding are underway. In the coming year, we will continue the dialogue on public cryptography and inaugurate its research program. An understanding of this issue at the senior levels of DoD and of the new administration will provide significant support to this NSA initiative.

[redacted] INTELLIGENCE SYSTEM

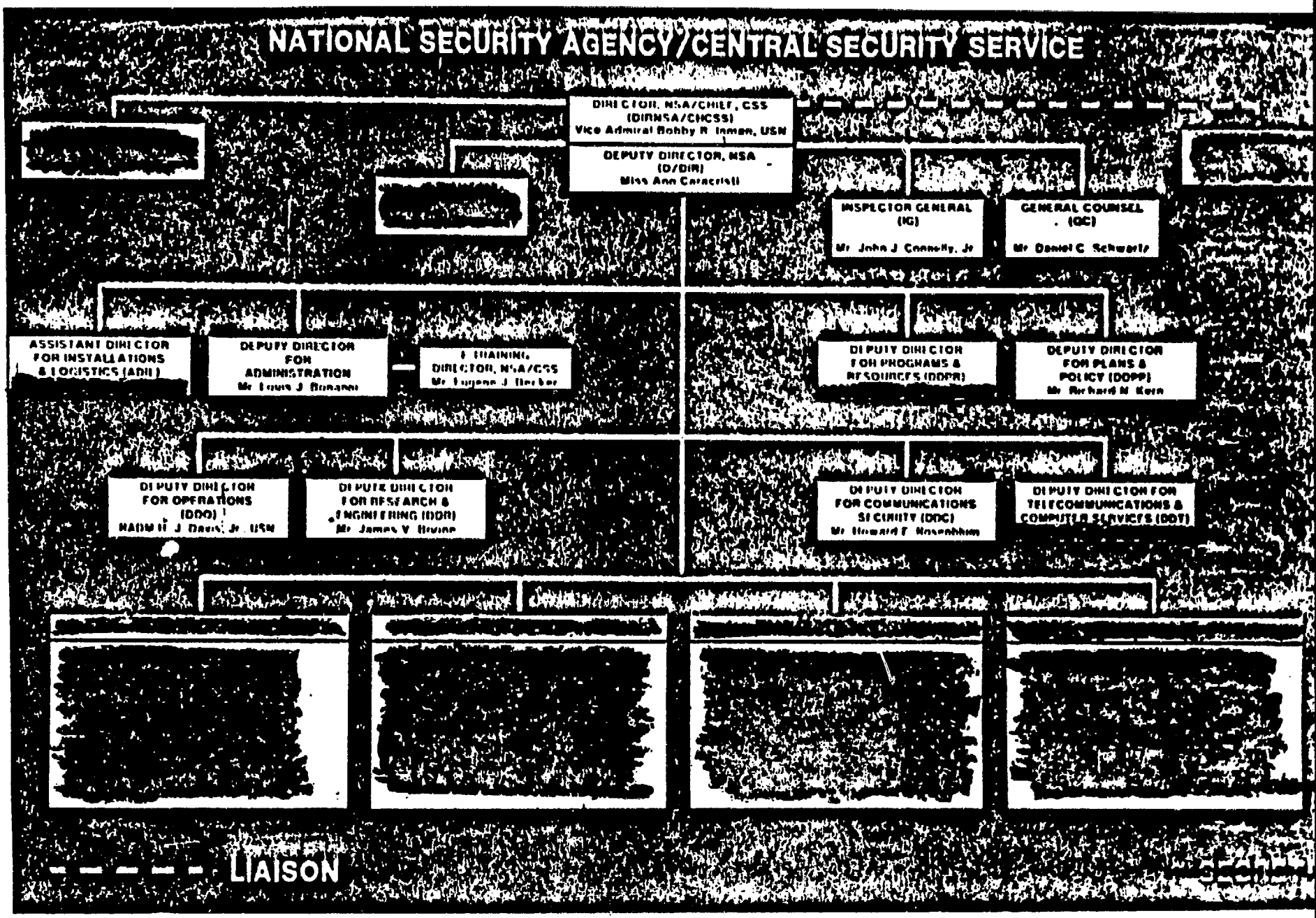
NSA has been an active participant in [redacted] study efforts and is committed to the initiative.

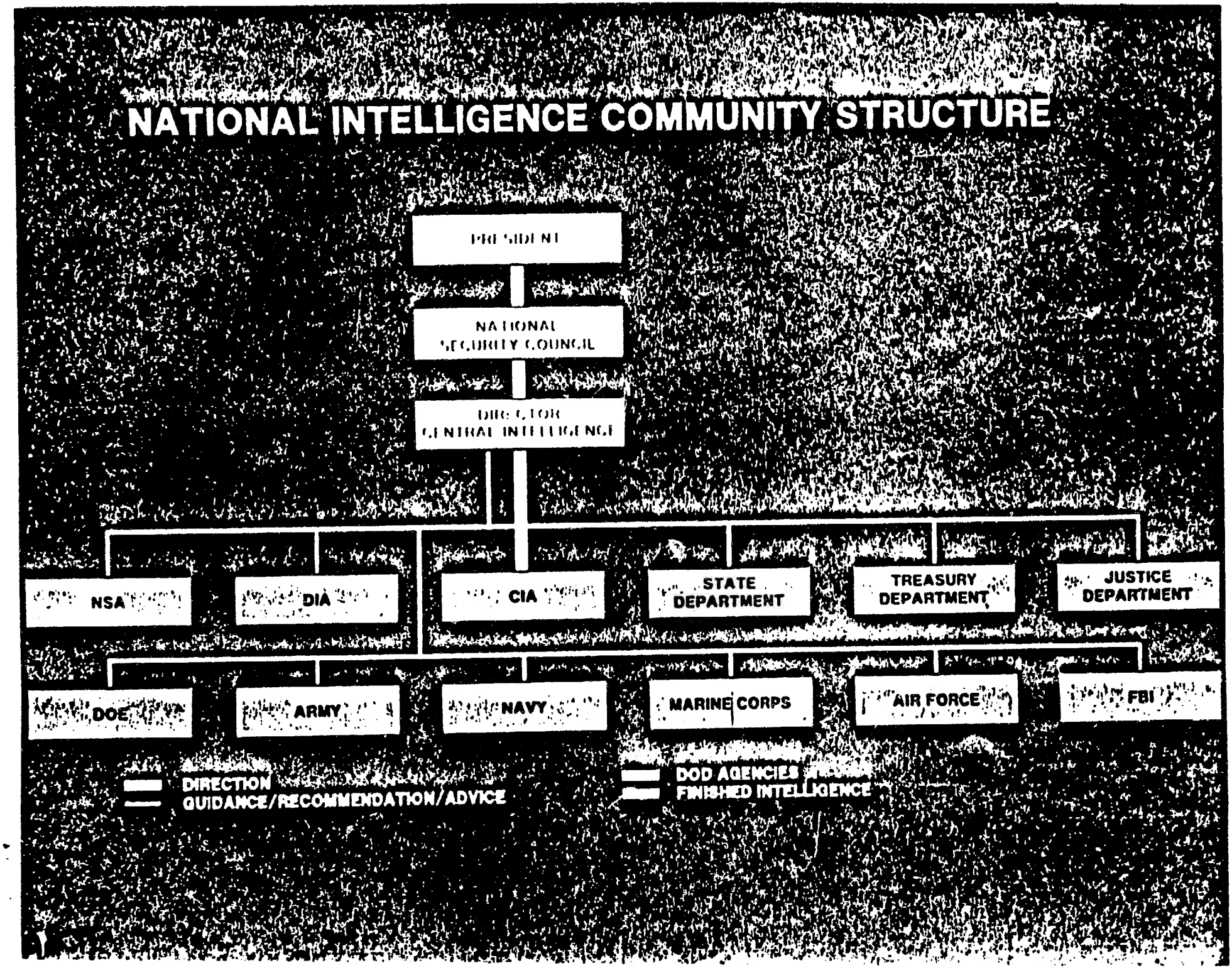
The [redacted] has, to date, emphasized determining the feasibility of [redacted] segments and, in August, directed that another year of definition study be accomplished. The emphasis will be placed on the [redacted] of the system concept. The NSA view as to how the [redacted] is proceeding was best expressed in a [redacted] memorandum to ASD(C^{3}I) and DUSD(PR). The Director, NSA referred to an [redacted] and stated, in part:

"...Your...memorandum essentially captures the findings of the [redacted] in their 18 August meeting, and I have little of substance to add. I would reemphasize, however, the great importance we place on the early definition of the concept of operations, especially the envisioned processing and staffing functions, and how they may influence the choice of options to be pursued. In this regard refinement of requirements, and the development of an operations concept must be undertaken if we are to acquire the desired end system.

I remain committed to the [redacted] initiative and look forward to continued participation in this effort."

[redacted]


NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
DIRECTOR, NSA/CHIEF, CSS (DIRNSA/CHCSS) Vice Admiral Bobby R. Inman, USN
DEPUTY DIRECTOR, NSA (D/DIR) Miss Ann Caracristi
INSPECTOR GENERAL (IG) Mr. John J. Connolly, Jr.
GENERAL COUNSEL (GC) Mr. Daniel C. Schwartz
ASSISTANT DIRECTOR FOR INSTALLATIONS & LOGISTICS (ADIL)
DEPUTY DIRECTOR FOR ADMINISTRATION Mr. Louis J. Rosano
TRAINING DIRECTOR, NSA/CSS Mr. Eugene J. Becker
DEPUTY DIRECTOR FOR PROGRAMS & RESOURCES (DDPR)
DEPUTY DIRECTOR FOR PLANS & POLICY (DDPP) Mr. Richard M. Kerr
DEPUTY DIRECTOR FOR OPERATIONS (DDO) RADM H. J. Davis, Jr., USN
DEPUTY DIRECTOR FOR RESEARCH & ENGINEERING (DDR) Mr. James V. Irvine
DEPUTY DIRECTOR FOR COMMUNICATIONS SECURITY (DDC) Mr. Howard F. Rosenblum
DEPUTY DIRECTOR FOR TELECOMMUNICATIONS & COMPUTER SERVICES (DDT)
LIAISON


NATIONAL INTELLIGENCE COMMUNITY STRUCTURE
PRESIDENT
NATIONAL SECURITY COUNCIL
DIRECTOR CENTRAL INTELLIGENCE
NSA
DIA
CIA
STATE DEPARTMENT
TREASURY DEPARTMENT
JUSTICE DEPARTMENT
DOE
ARMY
NAVY
MARINE CORPS
AIR FORCE
FBI
DIRECTION
GUIDANCE/RECOMMENDATION/ADVICE
DOD AGENCIES
FINISHED INTELLIGENCE