~~COMINT~~

~~SECRET//X1~~

NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE

TRANSITION 2001

DECEMBER 2000

Derived From: NSA/CSS Manual 123
Dated: 24 February 1998
Declassify On: X1

~~SECRET//X1~~

~~COMINT~~

(U) TABLE OF CONTENTS

TRANSITION 2001

(U) ORGANIZATION AND MANAGEMENT

(U) OVERVIEW

(U) INTRODUCTION

(U) The National Security Agency is the nation's cryptologic organization and as such, is charged with two primary missions - exploiting foreign communications, also known as Signals Intelligence (SIGINT), and protecting U.S. information systems, also called Information Assurance (IA).

(U) A high-technology organization, NSA is on the frontiers of communications and information technology and is also one of the most important centers of foreign language analysis and research within the Government.

(U) Founded in 1952, NSA is part of the Department of Defense and a member of the U.S. Intelligence Community. NSA supports military customers, national policymakers, and the counterterrorism and counterintelligence communities, as well as key international allies. Agency headquarters are located at Fort George G. Meade, Maryland, in the Baltimore-Washington corridor.

(U) RESEARCH

(U) NSA also has one of the U.S. Government's leading research and development (R&D) programs. Some of the Agency's R&D projects have yielded state-of-the-art technologies in the private sector. For example, NSA's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to the modern computer. NSA also broke new ground in computer storage devices, quantum computing, and semiconductor technology. Moreover, NSA holds world records in quantum cryptography, cryptographic design and biometrics, and public key cryptography and cryptanalysis.

(U) HISTORY

(U) SIGINT is a unique discipline with a long and storied past. SIGINT's modern era dates to World War II when the United States broke the Japanese military code and learned of plans to invade Midway Island. SIGINT is believed to have helped shorten the war by at least a year. Today, SIGINT plays a vital role in keeping our country's key decision-makers apprised of rapidly changing world events and in safeguarding U.S. personnel around the world.

(U) THE NSA WORK FORCE

(U) The NSA work force consists of highly talented military and civilian members with a wide array of skills and expertise: mathematicians, physicists, cryptanalysts, intelligence analysts, linguists, computer scientists, and engineers. In fact, NSA is said to be the largest employer of mathematicians in the United States and perhaps the world. This work force, combined with NSA's nationwide strategic alliance with a consortium of contractors and academia, has been the key to all past successes and remains our foundation for the future.

(U) EMERGING CHALLENGES

~~(C)~~ NSA continues to be challenged by an increasingly dynamic set of customer demands: transnational terrorism, narcotics trafficking, organized crime, counterintelligence, alien smuggling, asymmetric threats, and international disputes. Our military forces are more likely to be involved in coalition warfare, regional conflicts, peacekeeping operations, and nontraditional operations than in the past. At the same time, the rapid and unfettered growth of global information technology makes both of the Agency's missions harder—and more important—than ever. To meet these emerging challenges, NSA has embarked on an ambitious corporate strategy to transform its operations to a service-based architecture that includes a re-engineered cryptologic system with interoperability across the Community and common connectivity with our customers. This mandate for change firmly establishes SIGINT and Information Assurance as major contributors in ensuring information superiority of U.S. warfighters and policymakers.

(U) A PROUD TRADITION—A BRIGHT FUTURE

~~(S)~~ The National Security Agency has a proud tradition of serving the nation. NSA has been credited with preventing or significantly shortening military conflicts, thereby saving lives of U.S. military and civilian personnel. NSA gives the nation a decisive edge in policy interactions with other nations, in countering terrorism, and in helping stem the flow of narcotics into our country. NSA has been the premier information agency of the industrial age, and, through ongoing modernization and cutting edge research, will continue to be the premiere knowledge agency of the information age.

(U) MISSION STATEMENT

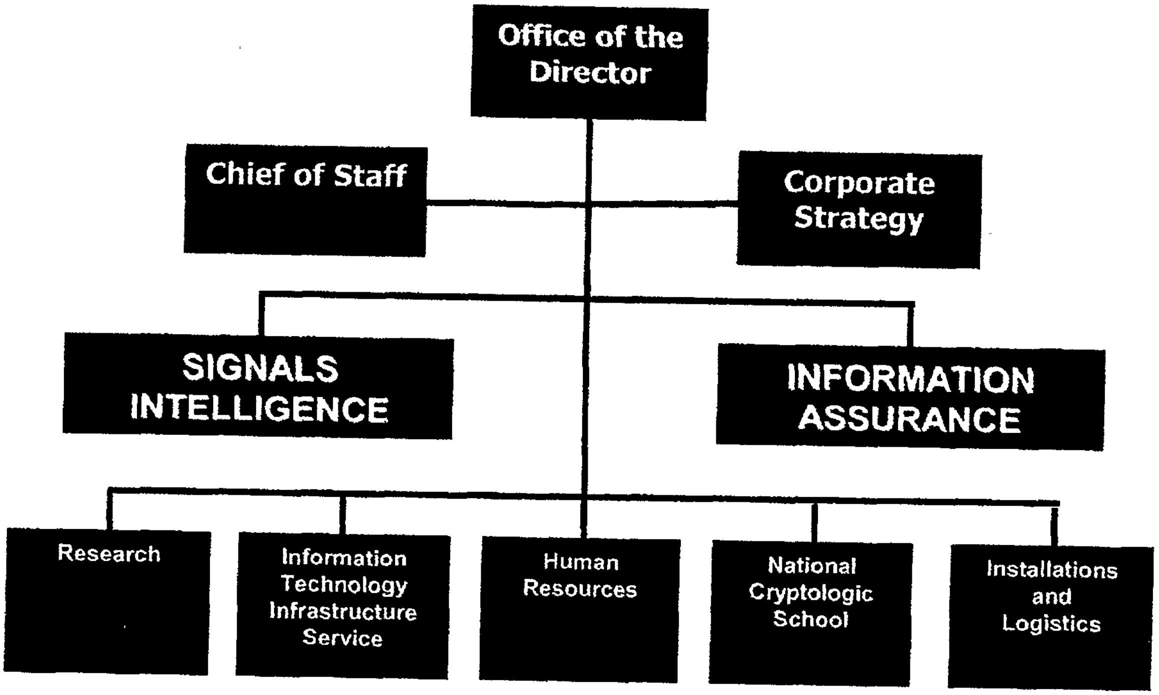
(U) INFORMATION SUPERIORITY FOR AMERICA AND ITS ALLIES

(U) Intelligence and information systems security complement each other. Intelligence gives the nation an information advantage over its adversaries. Information systems security prevents others from gaining advantage over the nation. Together the two functions promote a single goal: information superiority for America and its allies.

(U) ORGANIZATIONAL STRUCTURE

UNCLASSIFIED

National Security Agency/Central Security Service



UNCLASSIFIED

(U) GOALS

(U) BREAKTHROUGH GOAL: TRANSFORM THE CRYPTOLOGIC SYSTEM

(U) NSA/CSS must master and operate in the global net of tomorrow. To do so we must refine requirements; better understand and help inform customer expectations; and selectively disinvest some current operations to free up resources to modernize. In restructuring, NSA/CSS must assess risk, inform customers of lost capability, and quantify the growth in resources needed to sustain capability and reach a transformed state. We must inform our stakeholders of our intentions, strengthen our strategic alliances with our partners and together build the unified cryptologic architecture that will enable us, as a community, to meet the nation's needs.

(U) In transforming the cryptologic system, the NSA/CSS must shift significant emphasis and resources from current products, services, and targets to the modern and anticipated information technology environment for both SIGINT and Information Assurance. The NSA/CSS must be capable of operating with our partners seamlessly in the global network; where possible sustaining our global response; and when necessary succeeding through tailored access. We must create secure, agile and interoperable capabilities to provide our customers with desired information and security products and services in the modern environment, where we and our targets co-exist in the same global network. Only through greater collaboration and interoperability with partners can we move through the transformation period and achieve our end-state successfully.

(U) Our Information Assurance business must continue to rapidly change and grow. In the space of a decade our nation and our allies have become highly dependent on information systems to conduct essential business, including military operations, civil government, and national and international commerce. We must provide our increasingly diverse customer set emerging government and commercial off-the-shelf technologies and techniques to protect their information. We will also provide the highest level of protection to our SIGINT system. We will develop our newest line of business, Defensive Information Operations (DIO), so that we can assist customers in identifying, verifying, and responding to attack.

(U//~~FOUO~~) As our missions progress, synergy among professionals performing each mission will be of paramount importance to our overall success. The lines will blur between strictly SIGINT and INFOSEC disciplines and we will only survive if we learn to share all we know about the global network across our two missions and determine jointly how we provide pertinent intelligence and information assurance products and services to our customers.

(U) NSA/CSS strategic goals and objectives are structured to achieve this end-state, and its business plan will identify the specific shifts of resources, burdens and capabilities required to achieve those goals and objectives. Our overarching goal is transformation.

(U) GOAL 1

(U) Ensure responsive intelligence information and information assurance for national decision-makers and military commanders.

- (U) Collaborate with customers continually to refine needs and priorities and to identify the Unified Cryptologic System response within resource constraints.
- (U) Increase NSA/CSS ability to protect networked communications.
- (U) Maintain current protection posture in other environments, where resources permit.
- (U) Selectively increase production of information from the global network.
- (U) Sustain production of intelligence through global response, as resources permit.
- (U) In close collaboration with cryptologic and Intelligence Community partners, establish tailored access to specialized communications when needed.

- (U) Work with our customers to implement mission management systems for SIGINT and IA.

(U) GOAL 2

(U) Continuously modernize the cryptologic system by using advanced technology to provide solutions for the production and protection of information.

- (U) Deploy tools efficiently to sort, process, move and store information.
- (U) Deploy a modern, secure web-based analysis, reporting, and dissemination system.
- (U) Work with our partners to deploy mission management systems for SIGINT and DIO.
- (U) Achieve the Unified Cryptologic Architecture objectives of a common information infrastructure by establishing interoperability among cryptologic systems both internally and with those of customers and partners.
- (U) Ensure the availability of leading edge technologies and advanced mathematics through community, industry, and academic partnerships.
- (U) Deploy a robust, layered, and secure information technology infrastructure to support diverse communities of interest.
- (U) As resources permit, deploy technology to meet operational requirements in non-networked environments.

(U) GOAL 3

(U) Shape the NSA/CSS work force to meet SIGINT and Information Assurance mission challenges.

- (U) Build and sustain a diverse civilian, military (both active and reserve), and contractor work force with the right skill mix to respond to mission requirements.
- (U) Expand mission driven education, training, and career development to optimize individual and team performance to achieve our goals and objectives.
- (U) Increase intra- and interagency collaboration, including rotational assignments, training, and joint analysis and problem solving.
- (U) Apply personnel management techniques and reward performance and behaviors that ensure mission accomplishment and are linked to our goals and objectives.

- (U) Maintain a trusted work force through effective personnel security programs.
- (U) Provide equal opportunity in all human resource policies and practices, and safeguard employees' health, safety, and physical security.

(U) GOAL 4

(U) Maximize the use of resources through effective business processes and prudent risk to achieve and sustain Information Assurance solutions and responsive Signals Intelligence.

- (U) Reallocate and consolidate resources to achieve a transformed cryptologic system.
- (U) Strengthen partnerships within the cryptologic community to more efficiently exploit the global network.
- (U) Re-engineer internal business processes using best practices to maximize the return on investment for both missions.
- (U) Deploy a corporate management information system to enable better decision-making.
- (U) Implement effective systems engineering and disciplined program management as central components of our end-to-end modernization effort.
- (U) Pursue programmatic increases to accelerate the transformation of the cryptologic system and to meet the increasing requirements for Information Assurance solutions.
- (U) Understand and communicate NSA/CSS resource limitations.
- (U) Provide the NSA/CSS work force with the environment, systems, and facilities it needs to fulfill the NSA/CSS mission.

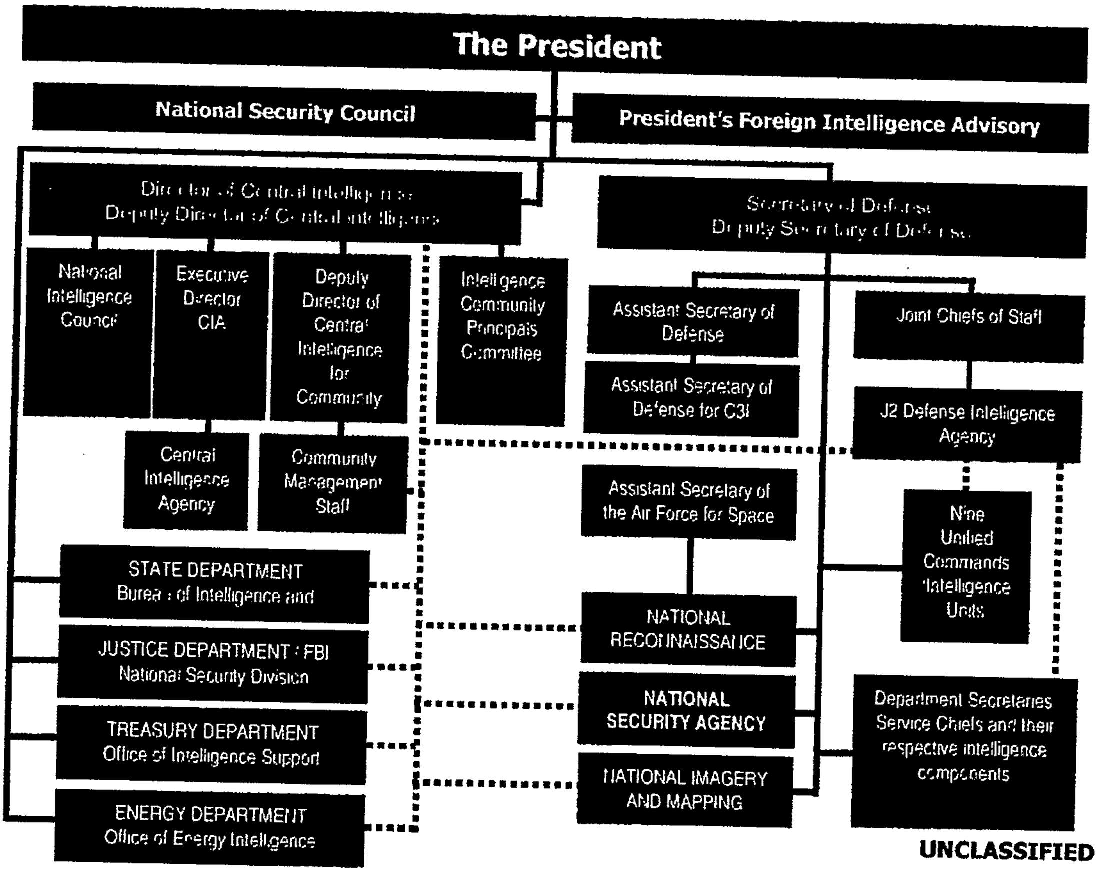
(U) MANAGEMENT

(U) CHAIN OF COMMAND

UNCLASSIFIED

NSA/CSS and the Intelligence Community

Dark lines in the chart below show a managerial relationship, while dashed lines show a budgetary or advisory relationship.


The President
National Security Council
President's Foreign Intelligence Advisory
Director of Central Intelligence
Deputy Director of Central Intelligence
National Intelligence Council
Executive Director CIA
Deputy Director of Central Intelligence for Community
Intelligence Community Principals Committee
Central Intelligence Agency
Community Management Staff
STATE DEPARTMENT Bureau of Intelligence and
JUSTICE DEPARTMENT : FBI National Security Division
TREASURY DEPARTMENT Office of Intelligence Support
ENERGY DEPARTMENT Office of Energy Intelligence
Secretary of Defense
Deputy Secretary of Defense
Assistant Secretary of Defense
Assistant Secretary of Defense for C3I
Assistant Secretary of the Air Force for Space
NATIONAL RECONNAISSANCE
NATIONAL SECURITY AGENCY
NATIONAL IMAGERY AND MAPPING
Joint Chiefs of Staff
J2 Defense Intelligence Agency
Nine Unified Commands Intelligence Units
Department Secretaries Service Chiefs and their respective intelligence components

UNCLASSIFIED

(U) REGULATORY AUTHORITY

(U) AUTHORITIES AND RESPONSIBILITIES OF THE DIRECTOR, NSA

(U) NSA was established pursuant to the 1952 Truman Memorandum. The Truman Memorandum recognized that communications intelligence activities of the U.S. are a national responsibility and designated the Department of Defense as the executive agent of the Government for the production of communications intelligence.

(U) NSA's missions and functions have been defined and enhanced in a series of Executive Orders (E.O.) and other documents, principally E.O. 12333, "United States Intelligence Activities," and National Security Council Intelligence Directive (NSCID) 6, "Signals Intelligence." E.O. 12333 describes the organization of the Intelligence Community and details the responsibilities of the heads of each Agency. NSCID 6 establishes NSA and spells out responsibilities and authorities of the Director, including some classified relationships that are not found elsewhere.

(U) In accordance with the Goldwater-Nichols DoD Reorganization Act of 1986, the Secretary of Defense (SecDef) designated NSA as a combat support agency with respect to certain combat support functions NSA performs.

(U) DIRNSA's relationship to other elements of the Executive Branch appears in the following authorities:

- (U) E.O. 12333, which makes DIRNSA responsible to the SECDEF (Paragraph 1.12) and also limits the conduct of SIGINT to NSA in accordance with guidance from the DCI; and
- (U) DoD Directive S-5100.20, "The National Security Agency and the Central Security Service," which generally promulgates the authorities of E.O. 12333 and NSCID 6, and prescribes DIRNSA's responsibilities within DoD. Through this Directive, SECDEF also delegates to DIRNSA certain administrative authorities.

(U) The Director, NSA's (DIRNSA's) authorities with respect to NSA's three missions of Signals Intelligence (SIGINT), Information Assurance (IA), Operations Security (OPSEC) and the Information Operations Technology Center (IOTC) flow from the following:

(U) SIGINT[1]

- (U) E.O. 12333, which generally charges DIRNSA with establishing and operating an effective unified organization for SIGINT activities. NSA is authorized to collect, process and disseminate signals intelligence information for national foreign intelligence purposes in accordance with guidance from the DCI; and

[1] (U) The Foreign Intelligence Surveillance Act (FISA), used principally by NSA and the FBI, regulates certain electronic surveillance activities in the United States to collect foreign intelligence, but does not specifically mention DIRNSA or the Agency.

- (U) NSCID 6, derived from the original Truman Memorandum, which describes the appointment process for DIRNSA and provides additional detail about the SIGINT mission itself. The SecDef is designated as executive agent of the Government for the conduct of SIGINT activities.

(U) INFORMATION ASSURANCE

- (U) E.O. 12333, which includes communications security among NSA's many responsibilities; and
- (U) National Security Directive (NSD) 42, "National Policy for the Security of National Security and Information Systems," which establishes DIRNSA as National Manager responsible for securing the Government's national security telecommunications and information systems[2].

(U) OPSEC

- (U) National Security Decision Directive (NSDD) 298, "National Operations Security Program," which designates DIRNSA as the Executive Agent for interagency OPSEC training and authorizes establishment of NSA's OPSEC program.

(U) INFORMATION OPERATIONS TECHNOLOGY CENTER

(U) The Director's authority as Executive Agent for the Information Operations Technology Center (IOTC) stems from a Memorandum of Agreement between the Department of Defense and the Intelligence Community established the IOTC as a joint activity of the Department of Defense and the Intelligence Community. DIRNSA has been designated as the Executive Agent (EA) for the operation of the IOTC. In his capacity as EA, DIRNSA, after consulting with the SecDef and the DCI, appoints a Director for the IOTC.

(U) MANAGEMENT STUDIES AND ISSUES

(U) Three management studies of the National Security Agency are provided in the appendix.

- (U) External Team Report, NSA, dated October 22,1999
- (U) New Enterprise Team (NETeam) Recommendations, NSA, dated 1 October 1999

[2] (U) The Computer Security Act of 1987 gives the National Institute of Standards and Technology (NIST) the responsibility to develop security standards for systems that handle unclassified information, while NSA retains responsibility for systems that process national security information.

- The National security Agency: Issues for Congress, CRS Report, dated November 17, 2000.

(U) These reports identified seven areas where NSA needed improvement: governance, ethos, vision, career development, resource management, intergovernmental communication, and strategy. NSA's response to these concerns have included the overhaul of NSA's leadership structure, the hiring of a Chief Financial Manager, Information Technology Officer and Senior Acquisition Executive from outside of the Agency, and the development of an agency-wide business plan.

(U) CHANGES IN GOVERNANCE

(U) NSA has completely transformed its organizational plan and its leadership team. This new team has fewer members, but they have more significant decision-making authority. NSA has also revitalized its NSA Advisory Board activities and is evaluating ways to reengineer the Central Security Service.

(U) CHANGES IN ETHOS

(U) The Director, NSA has enhanced his ability to communicate with and respond to NSA employees. The Director has established an e-mail address that allows employees to send messages directly to him. He has also established a variety of communication venues (DIRGRAMS, Television Programs, and Town Meetings) to ensure that his message is being communicated and that he is able to engage in an ongoing dialogue with the workforce.

(U) CHANGES IN VISION, MISSION AND STRATEGY

(U) By far the most dynamic changes undertaken by the Agency have been those associated with the articulation of NSA's Mission. To accomplish this task, NSA has formulated, and is implementing, a business plan, strategic plan and organizational realignment plan. These Plans are designed to help Agency leaders identify the Agency's goals, set priorities and focus on the core mission.

(U) CHANGES IN WORKFORCE AND CAREER DEVELOPMENT

(U) Government downsizing, NSA's inability to hire, and the reassignment process resulted in a work force with skills out of alignment with our mission needs. The Director has committed to focusing NSA's hiring program to its core mission areas. As a result, the hiring program has been significantly enhanced to allow the Agency to attract experts from the private sector. Additionally, directed assignments, tuition reimbursement programs and promotion board reforms have also been initiated to ensure that NSA remains capable of completing its mission.

(U) CHANGES IN RESOURCES MANAGEMENT

(U) This is an area in which the Agency is making rapid improvement. A zero-based review of all of our programs and projects to search out any overlap and identify those that could be consolidated or eliminated has been completed.

(U) In FY200, the Director created the positions of chief financial manager (CFM) and senior acquisition executive (SAE). Both of these positions are directly accountable to the Director and centralize resources and acquisition personnel.

(U) The CFM has been charged with a far-reaching portfolio of tasks. These include implementation of best, most current business practices, ensuring that resources decisions are aligned with mission planning and with creating a financial management information system as well as a system of performance measures. Under the CFM's direction, the Agency has produced its FY02-03 Business Plan (please see below).

(U) The SAE is working to redress specific criticisms in the external and internal reports. He is linking the requirements process with the acquisition and budget processes and is implementing acquisition policies and procedures that comply fully with public law and with Federal government guidance and regulations. He is developing standard procedures for Agency "make versus buy" decisions, and is the advocate for improved training of the acquisition workforce. The Agency already is exceeding its FY01 goals of increasing the proportion of competitive contracts from 66 to 80 percent of the total and of executing with credit cards 95 percent of purchases under $2,500.

(U) A new initiative for the Agency is a knowledge management program. We have begun to develop processes, relationships, and supporting technology to make the best use of our own expertise, and to reduce our "cost of not knowing."

(U) GROUNDBREAKER, the decision to outsource routine information technology functions, is strong evidence of the Agency's readiness to re-think the way it does its business and its acceptance of risk.

(U) CHANGES IN RELATIONSHIP BUILDING

(U) The Agency has gone far in transforming itself from the "No Such Agency" to an agency with a policy of active engagement with the news media and the public, an agency that provides timely, substantive information. The Director recognizes that he heads a powerful and secret agency in a country with a public that mistrusts power and secrecy. The Director himself frequently speaks at public fora. We stress that the Agency acts responsibly, and strictly complies with U.S. laws that protect the privacy of U.S. citizens. News media representatives were invited inside NSA along with the families of employees during last September's NSA Family Day.

(U) Where consistent with security concerns, the Agency has been active in declassification of documents and making them available to the public. The Agency has recently released significant intelligence documents on the Korean War.

(U) In addition to the news media and general public, the Agency has placed strong emphasis on building relationships with private industry and institutions and with other governmental bodies. The Agency has cooperated closely with state and local authorities in road construction and environmental affairs.

(U) In conjunction with our emphasis on the Agency acting as a good citizen, the Agency also has stressed relations with Congress. The Agency recognizes that Congressional buy-in is a necessary first step toward transforming the Agency, and has been keen to keep Congress fully and currently informed. Legislative oversight is a key source of public confidence in the Agency and the source of new funding that allows the Agency to meet its mission while at the same time it is Transforming.

(U) Cooperation with war fighters: The Director has briefed Agency transformation plans with the Commanders-in-Chief and explained our position on giving priority to modernization over current readiness and our increased reliance on both foreign partners and the military services' cryptologic elements.

(U) CHANGES IN BUSINESS PLANNING

(U) The Agency has just issued the FY02-03 Business Plan. Building on prior business and strategic plans, this is a single plan for both signals intelligence and information assurance missions, and serves as our guide for transformation over the next two years. It addresses four strategic issues: rebuilding analysis, countering strong encryption, enabling defense-in-depth for the nation, and implementing defense-in-depth at NSA/CSS.

(U) The signals intelligence portion of the Business Plan looks at programs and projects that may be reduced or eliminated in order to redirect money and resources into fundamental transformation. It builds on the actions and decisions of the signals intelligence plan drafted earlier this year and initiates new ones, mapping out specific goals. These decisions will not be easy, but they will be crucial to the Agency's future success. Similarly the information assurance portion of the business plan maps out NSA's role and contributions in the implementation of the defense in depth strategy. This strategy is designed to assure the availability of security products and services required to implement information assurance solutions for each of the Defense in Depth layers; to develop and support the operation of the security management and attack sensing, warning, and response infrastructures; as well as contributing to raising the level of information assurance training and awareness.

(U) EXTERNAL PROCESS

(U) NSA's outreach to external customers is crucial to the continued success of the Agency. Customer satisfaction is a key measure of our success. We use feedback to continuously improve our products and services and to anticipate future customer needs. We have expanded both the type of information we provide and the circle of customers to whom we distribute our product. This is of particular significance to U.S. and Allied commanders in the field as well as law enforcement and counterintelligence officials. We continue to increase our collaboration with customers and partners to enhance the value of our products for decision-makers throughout the Government.

(U) EXECUTIVE—KEY INTERAGENCY RELATIONSHIPS

(U) NSA works closely with the following Department of Defense and Intelligence Community Agencies:

- Director of Central Intelligence
- Ballistic Missile Defense Organization
- Joint Staff
- Community Management Staff
- Assistant Secretary of Defense for Command, Control Communications & Intelligence
- Defense Intelligence Agency
- Defense Security Service
- Defense Logistics Agency
- Department of the Army
- Department of the Navy
- Department of the Air Force
- Marine Corp
- US Coast Guard
- National Communication System
- Defense Information Systems Agency
- National Reconnaissance Organization
- Central Intelligence Agency
- National Imagery and Mapping Agency

(U) NSA also works with the following Civil Agencies and Executive Branch Offices to provide Signals intelligence and Information Assurance products and services in the form of intelligence reports and Defensive Information Systems Support:

- Executive Office of the President
- Department of State

- Department of Justice
- Department of Treasury
- Department of Energy
- Department of Commerce
- Department of Agriculture
- Drug Enforcement Agency
- Federal Bureau of Investigation
- Immigration and Naturalization Services
- Secret Service
- Judicial Branch
- Federal Emergency Management Agency
- Customs
- Bureau of Alcohol, Tobacco, and Firearms

(U) KEY MILITARY RELATIONSHIPS

(S//SI) ~~(U)~~ Support to Military Operations (SMO) is a key part of the NSA/CSS charter. As the Chief of the Central Security Service, the Director NSA is the senior U.S. SIGINT authority responsible for providing support to the following military customers:

- Joint Chiefs of Staff
- Commanders In Chief
    - Central Commands
    - European Command
    - Pacific Command
    - Joint Forces Command
    - Southern Command
    - Space Command
    - Special Operations Command
    - Strategic Command
    - Transportation Command
    - North Atlantic Treaty Organization
- Tactical Commands
- Service Cryptologic Elements

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

- North Atlantic Treaty Organization

(U) CONGRESSIONAL

(U) The Director of the National Security Agency is obligated by law to keep Congress "fully and currently informed of intelligence activities." The following are the primary oversight committees for NSA:

- Senate Select Committee on Intelligence
- Senate Appropriations Committee, Defense Subcommittee
- House Permanent Select Committee on Intelligence
- House Appropriations Committee, Defense Subcommittee

(U) NSA also interacts with:

(b) (1)
(b) (3)-P.L. 86-36

- Senate Armed Services Committee
- House International Relations Committee
- House Appropriations Committee, Surveys and Investigations Team

(U) FY2001 CONGRESSIONAL LANGUAGE HIGHLIGHTS

(U) SSCI Mark:

- (S) Plus-up of [redacted]ew money).
- (S) "Churned" [redacted]to support NSA Business Plan in information technology backbone and SIGINT modernization efforts.
- (U) Advocates DIRNSA having greater authority over planning, programming, budgeting, and execution of entire SIGINT budget.

(U) HPSCI Mark

- (U) No new money
- (U) Supports NSA business plan as one of its top priorities, extensive churn within CCP reflecting Committee's endorsement of plan.
- (U) Directs DCI System Acquisition Executive to review major NSA modernization acquisitions, and confirm readiness to proceed.

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U) SSCI-HPSCI Conference

- (S) Authorized [redacted] positions for the CCP Program.
- (S) Authorized [redacted] f FY00 funds appropriated by prior year supplemental appropriations act.
- (U) Concerned about implementation of acquisition reforms, hiring of commercial management consultants, information technology backbone, systems engineering, and modernization efforts.
- (U) Noted slow progress on defining the Unified Cryptologic Architecture.
- (U) Requested over 20 reports and briefings on various NSA activities and Congressionally directed actions.

(U) SAC-HAC Conference

- (S) Appropriated [redacted] for the CCP Program.

[redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

- (U) Supported parts of NSA Business Plan

(U) CRITICAL REPORTS TO CONGRESS

- (U) "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance"—published and disseminated to Intelligence Committees in February 2000
- (U) Responses to Congressionally Directed Actions (approximately 30 per year)
- (U) Congressional Notifications (71 in CY00)—formal notification required to keep Congress fully and currently informed on relevant issues of significant intelligence achievements and failures or illegal activities

(U) PENDING LEGISLATIVE ISSUES

(U) Encryption Exports

(U//~~FOUO~~) Any legislation affecting the controls on exports of encryption products is of high concern to NSA. NSA played an integral part in the announcement of new Administration regulations in this area during the 106th Congress, which had the effect of stopping potentially harmful bills sponsored by Sen. McCain and Rep. Goodlatte. Efforts by Senators Gramm and Enzi to overhaul the entire U.S. export control system, including encryption exports, by reauthorizing the Export Administration Act failed in the 106th Congress, and they are likely to try again in the 107th.

(U) Electronic Surveillance

(U//~~FOUO~~) It is very likely the 107th Congress will continue to investigate the issues of electronic surveillance and privacy, both in the areas of commerce and law enforcement and possibly foreign signals intelligence. At an open hearing before the House Intelligence committee in April 2000 on NSA's electronic surveillance activities, the Director, NSA and the DCI testified that NSA operates under the rule of law and does not commit industrial espionage. However, the FBI's introduction of a new electronic surveillance tool called CARNIVORE led to hearings and legislation on the use of the tool in a law enforcement or national security investigation. At the close of the 106th Congress, no legislation that would harm NSA's collection was enacted.

(U) Information Security Issues

(U//~~FOUO~~) Information security topics will continue to be a primary concern in the 107th Congress. Any legislation in this arena may affect NSA's information assurance mission. Also, legislation protecting national critical information infrastructures, promulgating information assurance practices, or creating a federal Chief Information Officer is expected.

(U) Personnel Legislation

(U//~~FOUO~~) The FY01 Intelligence Authorization Act authorizes NSA to establish a program for early retirement and separation pay in order to encourage employees to separate from service voluntarily. This program will be used in conjunction with the DoD Voluntary Early Retirement Authority in the FY01 DoD Authorization Act. NSA is seeking legislative authority to update its recruiting practices by authorizing the reimbursement of actual expenses involved in the recruitment process.

TRANSITION 2001

(U) BUDGET

(U) BUDGET OVERVIEW

~~(FOUO)~~ NSA is both an Agency of the Department of Defense and a component of the National Foreign Intelligence Program (NFIP). Agency budget authority is derived from both sources.

(U) DEPARTMENT OF DEFENSE

- (U) Information Systems Security Program (ISSP)
- (U) Defense Cryptologic Program (DCP)
- (U) Defense Airborne Reconnaissance Program (DARP)
- (U) Defense Counterdrug Intelligence Program (DCIP)

(U) NATIONAL FOREIGN INTELLIGENCE PROGRAM (NFIP)

- (U) Consolidated Cryptologic Program (CCP)

(U//~~FOUO)~~The mission of NSA/CSS is to provide and protect the nation's vital information. This mission is accomplished through the science of cryptology and incorporates two core disciplines Signals Intelligence (SIGINT) and Information Assurance (IA). SIGINT derives intelligence information by exploiting foreign communications and non-communications emitters. Information assurance is the protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit. NSA resources to accomplish these missions, including the corresponding resources of the Service Cryptologic Elements (SCEs), are summarized in the "Budget Detail" section below. These resources include the costs to sustain ongoing SIGINT and Information Assurance operations, to develop and deploy new capabilities to sustain continuity against cryptologic targets and technology changes, the cost of civilian and military manpower, and new investment required to achieve cryptologic transformation.

(U) The key drivers for NSA budget development are:

- (U) Joint Vision 2020 for the Department of Defense;
- (U) The Director of Central Intelligence Strategic Intent for the U.S. Intelligence Community;
- (U) The NSA/CSS National Cryptologic Strategy for the 21st Century; and
- (U) The annual NSA/CSS Business Plans.

~~(S)~~The NSA/CSS Business Plan focuses internal development of the Agency budget. The corporate NSA business planning process has focused, for the last two budget cycles (FY01-05 and FY02-07), on transformation of the Cryptologic System. For the Consolidated Cryptologic Program (CCP) the strategic budget emphasis has been on accepting increased risk to current SIGINT operations in an effort to identify funding for the most urgent transformation requirements. These requirements include SIGINT access, countering the worldwide proliferation of strong encryption, rebuilding SIGINT analysis, modernizing the cryptologic information technology infrastructure, and protecting NSA information and information systems. The information assurance focus continues to be on development of an active cyber defense capability to protect sensitive U.S. information, detecting and reporting intrusions into information systems, and responding to these attempted intrusions.

~~(S)~~ In the last two budget cycles NSA has internally realigned resources totaling some [redacted] across the five year defense plan to fund the most urgent corporate transformation requirements. To this end, NSA has cut civilian personnel by an additional 7.5% beginning in FY01 and 10% military personnel in FY02, terminated SIGINT field sites, consolidated mission and support activities/operations, stopped legacy development programs, and realigned strategic funding relationships with SIGINT partners. Beyond NSA, the Intelligence Community and Congress have demonstrated a considerable interest in cryptologic transformation, increasing NSA's total budget authority in the key mission areas of SIGINT access, cryptanalysis, management of the cryptologic mission, the information technology infrastructure, and intrusion detection. This internal NSA realignment and the external increases *notwithstanding, cryptologic transformation continues to be significantly* underfunded. Transformation-related overguidance for NSA totals some [redacted] in FY02 and [redacted] across the FYDP (see the "Budget Issues" section below).

(U//F~~OUO~~) NSA is also effecting transformation through reengineering internal organizations and processes. Key functional managers have been hired from outside of NSA, and we will begin to outsource functions previously done in-house. The Agency is instituting and strengthening business processes and modifying its organizational structure. And, NSA has begun to implement a service-based architecture that will allow cryptologic operations in a network of service domains. The NSA budget request for FY 2002, which will be submitted as part of the President's budget request to the new Congress, enables the Agency to meet the near-term goals of the FY 2002-2003 NSA/CSS Business Plan, maintains essential readiness, and continues the Cryptologic System focus on transformation.

(b)(1)
(b)(3)-P.L. 86-36

(U) BUDGET DETAIL

~~(S)~~ The following information provides a summary of NSA resources, including those of the SCEs. One should be mindful that the following summary represents the SIGINT and Information Assurance resources that are directly controlled by the Director, NSA. There are additional SIGINT and Information Assurance resources in the NFIP and DoD that reside in budgets external to NSA [redacted] The Director, NSA, "influences" these external resources through established Cryptologic Community processes. The Budget Detail that follows represents the FY02-07 NSA Budget Estimate Submissions.

~~SECRET~~

($'s Millions)	[redacted]
Consolidated Cryptologic Program (CCP)	
Information Systems Security Program (ISS	
Defense Cryptologic Program (DCP)	
Other DoD Programs (DCIP)	
Total NSA Dollars	

(# of Billets; Includes SCEs)	FY01	FY02	FY03	FY04	FY05	FY06	FY07
Civilian	18945	16753	16390	16335	16382	16382	16382
Military	[redacted]						
Total NSA Billets							

~~SECRET~~

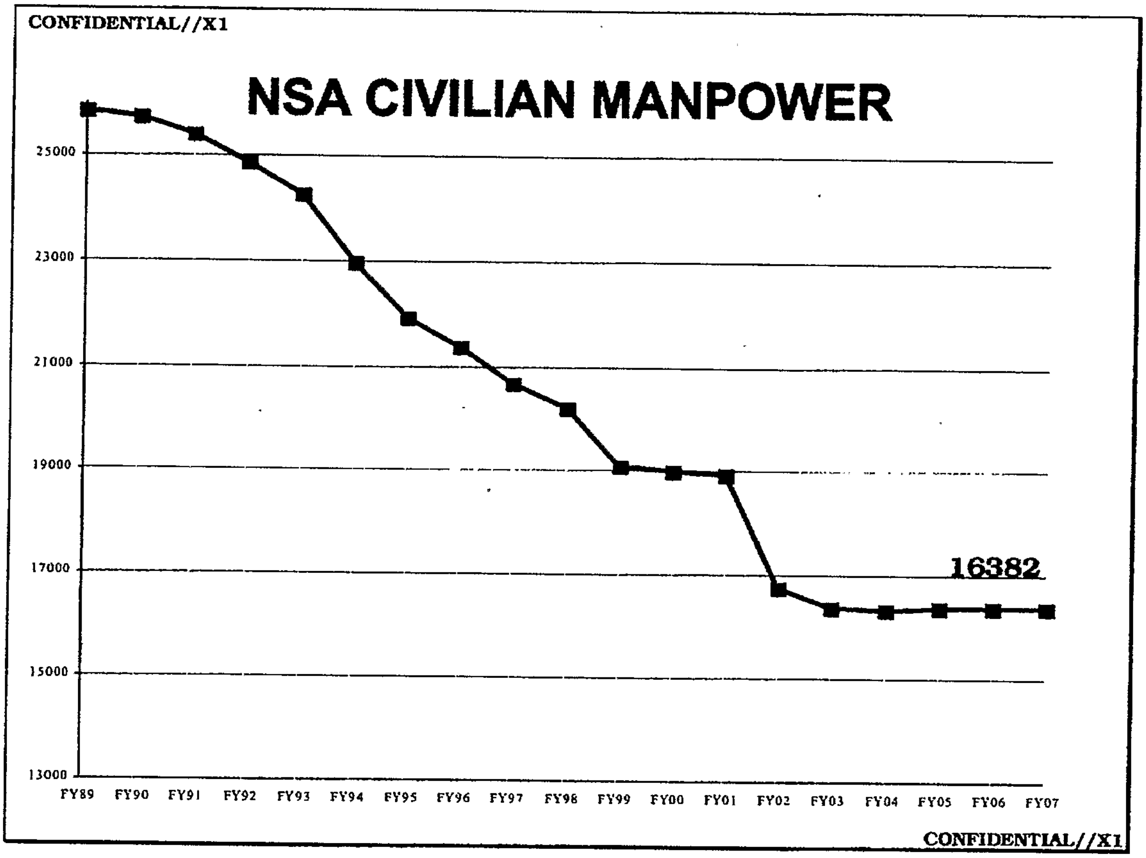
(b)(1)
(b)(3)-P.L. 86-36

(U) BUDGET TRENDS

(U) Below is a set of graphs portraying NSA funding and manpower trends over the last several years, and through FY07. Figure 1 reflects the CCP in constant dollar terms (i.e., buying power) since FY1987. Figure 2 shows the trend in NSA civilian manpower since FY 1989. Figure 3 reflects the same for military manpower. Lastly, Figure 4 summarizes funding for NSA's ISSP and DCP programs.

(U) Figure 1

(b)(1)
(b)(3)-P.L. 86-36


CONFIDENTIAL//X1
NSA CIVILIAN MANPOWER
25000
23000
21000
19000
17000
15000
13000
16382
FY89
FY90
FY91
FY92
FY93
FY94
FY95
FY96
FY97
FY98
FY99
FY00
FY01
FY02
FY03
FY04
FY05
FY06
FY07
CONFIDENTIAL//X1

(U) Figure 2

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(U) Figure 4

(U) BUDGET ISSUES

~~(S)~~ NSA budget issues center on cryptologic transformation. In many respects U.S. national security makes this transformation process urgent. In the end cryptologic transformation translates to funding. Sustaining essential current operations required to meet priority customer intelligence requirements, investing in critical transformation for the future, and doing both in the timeframe required to maintain target continuity, [redacted] Advanced capabilities that are needed today, particularly in the SIGINT analytic process. [redacted] as currently funded. [redacted] [redacted] A summary of NSA's specific overguidance requirements follows:

(b)(1)
(b)(3)-P.L. 86-36

~~SECRET//X1~~

	Prioritized CCP
1	Trailblazer
2	Systems Engineering
3	LIA
4	Access and Collection -1
5	Facilities Infrastructure
6	Human Resources
7*	Cryptanalysis (CA)
8	CMM
9	Weapons & Space (ELINT)
10	ITB
11	Access and Collection -2
12	Altruism
	Subtotal
	ISSP
	Total

[redacted]

*CA moves to priority 3 in FY03-7, bumping others down one position

~~SECRET//X1~~

Additional Information on each of the above categories

CCP-1	Allows delivery of program goal to achieve 3 missions and 6 sites by FY04
CCP-2	Allows execution of complete Sys. Eng. Plan for our transition to a Service-based Architecture
CCP-3	LIA=Language Viability/Dissemination -Sr. Language Authority Initiatives, language tools, TESTAMENT
CCP-4	Includes new access programs and HF
CCP-5	Upgrades/repairs to support transformation efforts including modernizing IT Backbone
CCP-6	Supports leadership development & web-based training in signals analysis, ELINT, FISINT, etc.
CCP-7	Increases computer processing capability, research, field initiatives
CCP-8	Cryptologic Mission Management-Develop architectural & Sys. Eng. Plans in single coherent CMM arch
CCP-9	Rebuild Technical SIGINT -Develop architecture; modernize tools & technology, dissemination, databases
CCP-10	ITB=Information Technology Backbone-extends modernization to field, upgrades JCS OPLANS to C2/C1
CCP-11	Includes additional access programs see CCP4
CCP-12	Expands partnerships, fully funds an aggressive strategy
ISSP	Includes Cryptomodernization, Attack Sensing, Warning, & Response, and Information Assurance Solutions

(b)(1)
(b)(3)-P.L. 86-36

TRANSITION 2001

(b)(1)
(b)(3)-P.L. 86-36

(U) PERSONNEL

(U) NSA/CSS WORK FORCE

~~(C)~~ The success of NSA/CSS is wholly dependent upon its people. That is as true for the future as it has been in the past. NSA and its military components must attract, train, develop, and retain people with the technical and analytic skills necessary to do our future missions. NSA's civilian population is now at an historical peak in terms of overall cryptologic skills. People hired in the 1970s and 1980s now comprise the backbone of the Agency's work force and bring to bear extraordinary skills on today's challenges. Due to mandated downsizing and resource restraints during the 1990s, NSA has been unable to hire enough people to replace the current work force as it moves into retirement. NSA plans to hire about 600 people per year beginning in FY01 in an attempt to correct the coming skills mix imbalance created by the pending retirement of analysts, linguists, and technical people hired 20-30 years ago. Outdated government compensation guidelines make it difficult to compete for top talent in today's highly competitive marketplace. In response, NSA has embarked on a compensation reform initiative that will lead to piloting a new compensation system in FY02. Already in FY01, recruitment bonuses are being paid for certain skills and the awards and promotion system is being revised to focus current compensation more on performance than it has been in the past. Simultaneously, NSA is launching a new skills management architecture that will improve skills alignment with mission requirements, enhance employee career development, and pave the way for the new compensation system.

~~(C~~ [redacted]nilitary members of the service cryptologic elements (SCEs) are full partners in the cryptologic effort, supplying just over half of the NSA/CSS workforce. The services have several initiatives underway to more effectively manage a force that has been suffering from poor retention and increasing numbers of first-term inexperienced personnel. The Agency is in the initial stages of a management engineering assessment to accurately determine required personnel strengths and skill sets.

(U) SUMMARY OF STATISTICS

~~(C)~~ CIVILIAN WORKFORCE DEMOGRAPHICS (START FY2001)

▪ ~~(C)~~ Total	17,129
▪ (C) Full Time	[redacted]
▪ (C) Part Time	
▪ ~~(C)~~ Civilian Location	
▪ ~~(C)~~ Headquarters	[redacted]
▪ (C) Deployed	

- (U//~~FOUO~~) Total Reductions Since FY 1993 24%
- (U//~~FOUO~~) Reduction to Support Population 28%
- (U//~~FOUO~~) Reduction to Mission Population 12%
- (U//~~FOUO~~) 11% of the workforce is eligible for regular retirement
- (U//~~FOUO~~) 19% of the workforce will be eligible for early retirement in FY 01
- (U//~~FOUO~~) 55% of the workforce FY2001 is in the relatively portable FERS retirement compared to 32% in FY88.
- (U//~~FOUO~~) 54% of the workforce has between 10 and 20 years of service
- (U//~~FOUO~~) 14% of the workforce has less than 10 years of service. (Compares to 49% of the workforce with less than 10 years service in FY88)
- (U//~~FOUO~~) After many years of relatively low attrition rates, NSA has seen resignation rates for Computer Scientists and Engineers increase sharply since FY98.

(U) MILITARY POPULATION (AS OF 19 DEC 00)

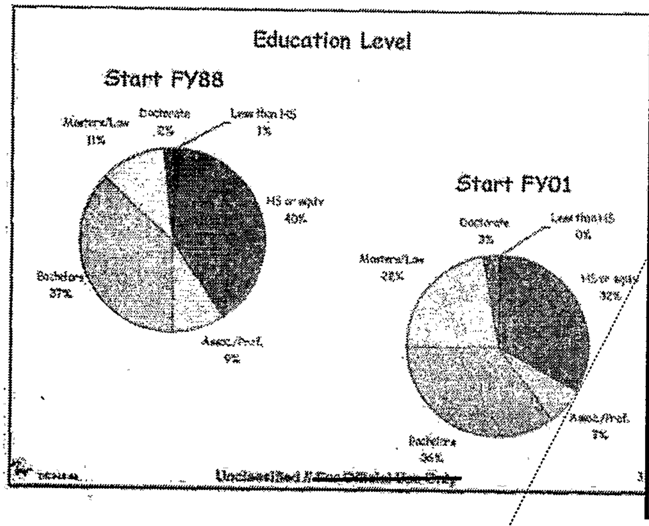
~~CONFIDENTIAL//X1~~

		%
ARMY	[redacted]	77%
NAVY	[redacted]	91%
MARINES	[redacted]	92%
AIR FORCE	[redacted]	92%
TOTAL	[redacted]	88%

~~CONFIDENTIAL//X1~~

(b)(1)
(b)(3)-P.L. 86-36

(~~U~~) Human resources summary slides follow.


Education Level

Unclassified // ~~For Official Use Only~~

[redacted]

[redacted]

(U//~~FOUO~~) NSA has a highly educated workforce. The number of personnel with graduate and doctorate degrees has risen by 50% since FY88.

(U//~~FOUO~~) 11% of the workforce is eligible for regular retirement–19% will be eligible for early retirement in FY 01.

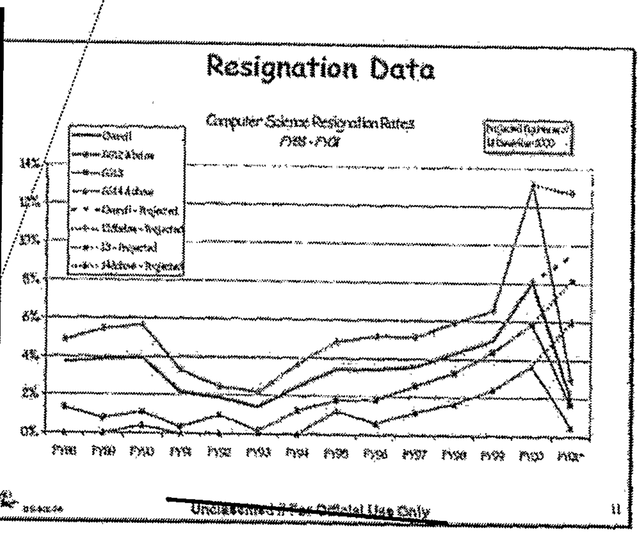
(~~C~~) The National Security Agency has been undergoing civilian downsizing, decreasing from well over 22,000 full time civilians in FY89 to just over 16,000 today.

(~~C~~) 54% of the civilian workforce has between 10 and 20 years of service. Unless this is addressed through a combination of hiring and managed attrition we will see a severe loss to our workforce when this group retires, compounded by an upward trend in technical skill resignations

(b)(1)
(b)(3)-P.L. 86-36

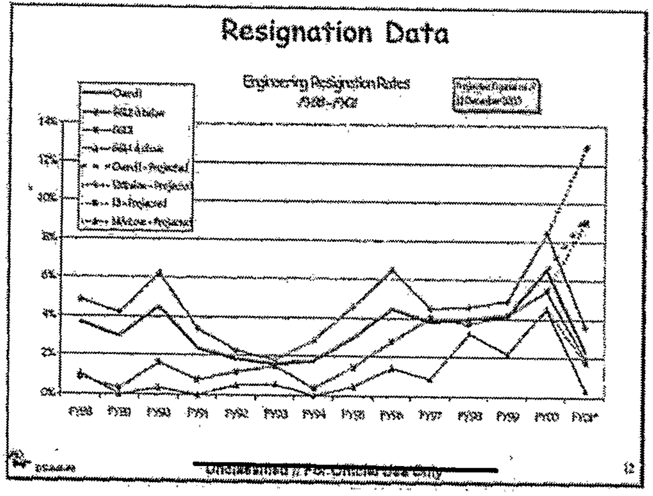
(b)(1)
(b)(3)-P.L. 86-36

[redacted]



Resignation Data

Computer Science Resignation Rates FY88 - FY01



Resignation Data

Engineering Resignation Rates FY88 - FY01

(U//~~FOUO~~) Hiring in the 1980s is largely sustaining the Agency today. Unfortunately there are few people following the1985-88 cohort to sustain us into the future.

(U//~~FOUO~~) Resignation rates for computer scientists at all grades continue to climb. The Computer Scientist resignation rate is more than double the Agency average and five times that of the analytic skill fields.

(U//~~FOUO~~) Resignation rates for engineers at all grades continue to climb. The Engineering resignation rate is double the Agency average and 4 times that of the analytic skill fields. Of note, approximately half of the computer scientists, mathematicians and engineers who resigned from the Agency in FY99 are now working for NSA contractors.

(U) PERSONNEL MANAGEMENT ISSUES

(U) RECRUITING & HIRING

(U) The Challenge

(U) Attract, train, develop, and retain people with the technical and analytic skills necessary to do our future missions.

(U) The Response

- ~~(S)~~The FY2001 hiring goal is 600, including a congressional plus up of 56.
- Targeted on technical skills in support of core Mission: computer science; engineering and physical science; information systems security; intelligence analysis; math.
- (U) In September 2000 created, elevated, and empowered the Office of Recruitment and Hiring to undertake the most intensive hiring program the Agency has had in many years.
- (U//~~FOUO~~) New compensation reform initiative will lead to piloting a new compensation system in FY02.
- (U) Streamlined and consolidated applicant processing.
- (U) Heavy investment in recruitment initiatives:
  - (U//~~FOUO~~) Expanded use of hiring bonuses in FY2001 for certain skills
  - (U) Increased our recruiting budget
  - (U) Expanded the size of the recruitment office
  - (U//~~FOUO~~) Continued the use of educational reimbursement programs that include employment obligations

COMINT

~~SECRET//X1~~

Transition 2001

COMINT

~~SECRET//X1~~

(U) POLICY/ISSUES

(U) POLICY DEVELOPMENT PROCESS

(U//~~FOUO~~) Policy development at NSA/CSS is the responsibility of the Director of Policy, who leads the NSA Office of Policy and reports to the NSA Chief of Staff. The Chief of Staff reports to the Director of NSA.

(U//~~FOUO~~) The Office of Policy ensures that NSA/CSS complies with and implements national, DoD and Director of Central (DCI) Intelligence policy, as appropriate. This is done through the NSA/CSS policy directive system, the United States Signals Intelligence Directive (USSID) system, and for human resources issues, through Personnel Management Memoranda. The Office of Policy oversees all policy development within NSA, and advises the Director on policy issues affecting NSA's signals intelligence and information assurance missions. The Office also oversees and supports NSA participation in external policymaking activities, such as the DCI's Policy Advisory Group, the Intelligence Community Principals and Deputies Committees, and the Military Intelligence Board.

(U) MAJOR POLICY ISSUES

(U) NATIONAL SECURITY AGENCY: RELEVANCE OF EXISTING AUTHORITIES IN THE INFORMATION AGE

(U) The National Security Agency is prepared organizationally, intellectually and -- with sufficient investment -- technologically, to exploit in an unprecedented way the explosion in global communications. This represents an Agency very different from the one we inherited from the Cold War. It also demands a policy recognition that NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist.

~~(C)~~ In the past, NSA operated in a mostly analog world of point-to-point communications carried along discrete, dedicated voice channels. These communications were rarely encrypted, and those that were used mostly indigenous encryption that did not change frequently. Before the arrival of fiber optic technology, most of these communications were in the air and could be accessed using conventional means; the volume was growing but at a rate that could be processed and exploited.

~~(C)~~ Now, communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less. Today, there are fiber optic and high-speed wire-line networks and most importantly, an emerging wireless environment that includes cellular phones, Personal Digital Assistants and computers. Encryption is commercially available, growing in sophistication, and packaged in off-the-shelf computer software. The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive missions, NSA must "live on the network."

~~(C)~~ NSA must respond quickly and comprehensively to the rapid deployment of new information technology into global networks. The volume, velocity and variety of information today demands a fresh approach to the way NSA has traditionally done its business. This new approach is well under way. Significant effort and investment are being applied to mastering the global network, both to protect our nation's communications and to exploit those of our targets. This new model for eSIGINT and for information assurance in the Information Age may require a restatement and endorsement of the policies and authorities that empowered the NSA in the Industrial Age.

(U) NSA's existing authorities were crafted for the world of the mid to late 20th Century, not for the 21st Century. Created by the Truman Memorandum of 1952, NSA's foreign intelligence (SIGINT) authorities stem from National Security Council Directive 6 of 1972, and Executive Order 12333 of 1981. Its Information Assurance authorities also derive from Executive Order 12333 which discusses Communications Security (COMSEC) which principally involved the building of security boxes for point-to-point communications. National Security Directive 42 of 1990 established the Director NSA as the national manager for national security information and information systems security (INFOSEC).

~~(S)~~ Entering the 21st Century, global networks leave the US critical information infrastructure more vulnerable to foreign intelligence operations and to compromise by a host of non-state entities. This vulnerability extends beyond classified and national security networks to the private sector infrastructure on which all depend. At the same time, because of the communications environment described above, availability of critical foreign intelligence information will mean gaining access in new places and in new ways. [redacted]

~~(S)~~ SIGINT in the Industrial Age meant collecting signals, often high frequency (HF) signals connecting two discrete and known target points, processing the often clear text data and writing a report. eSIGINT in the Information Age means seeking out information on the Global Net, using all available access techniques, breaking often strong encryption, again using all available means, defending our nation's own use of the Global net, and assisting our warfighters in preparing the battlefield for the cyberwars of the future. The Fourth Amendment is as applicable to eSIGINT as it is to the SIGINT of yesterday and today. The Information Age will however cause us to rethink and reapply the procedures, policies and authorities born in an earlier electronic surveillance environment.

(U/~~FOUO~~) Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment and all applicable laws. But senior leadership must understand that today's and tomorrow's mission will demand a powerful, permanent presence on a global telecommunications network that will host the "protected" communications of Americans as well as the targeted communications of adversaries.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

(U) GROUNDBREAKER

(U) Issue

(U) NSA intends to outsource its Information Technology (IT) infrastructure. The final decision will be made after contractor proposals are evaluated and a determination is made on the advantages to outsource rather than keep the work in house. The acquisition would represent a multi-billion dollar investment over its 10-year contract term.

(U) Discussion

- ~~(C)~~To deal with unprecedented volumes of information, NSA must change its approach to signals intelligence collection, processing, and dissemination. In short, NSA must build a modern information infrastructure that in many respects mirrors the technology and capabilities available on the global digital communications network.

- ~~(S)~~ The need for action was underscored in January 2000 when NSA experienced a catastrophic network outage for 3 ½ days. This outage greatly reduced the signals intelligence information available to national decision makers and military commanders. As one result, the President's Daily Briefing—60% of which is normally based on SIGINT—was reduced to a small portion of its typical size.

- (U//~~FOUO~~) Project GROUNDBREAKER is an NSA initiative to outsource the non-mission support areas of its IT infrastructure. NSA intends to pursue a government-industry partnership in four IT areas: distributed computing; enterprise and security management; internal networks; and telephony.

- (U) After completion of a Feasibility Study, in June 2000, NSA developed a draft Request for Proposal (RFP) that was distributed to three industry teams in October. The purpose of the draft RFP was to allow the vendors an opportunity to make comments and request further information before the final RFP is released. The final RFP will be released in January 2001, with contract award slated for July 2001. After the contract is signed, NSA's IT infrastructure would be run by a combined government-contractor team beginning in January 2002.

- (U) DoD is engaged at the level of the Deputy Under Secretary of Defense for Installations in pursuit of an exemption for GROUNDBREAKER from OMB Circular A-76, "Performance of Commercial Activities."

(U) Way Ahead

- (U) NSA is ready to update the incoming ASD/C3I at any time on the GROUNDBREAKER program.

- (U) After contract award, this will be a good opportunity for DoD to underscore the value of outsourcing non-core functions, even in sensitive areas like intelligence.

(U) POTENTIAL CYBER-INCIDENT

(U) Issue

(U) DoD experienced over 22,000 cyber attacks in CY1999. Most of these attacks had a negligible impact on operations. A handful were determined to have been perpetrated by sophisticated and determined adversaries. During the Presidential transition period a major cyber-attack is possible that would require the combined and coordinated resources of the entire Computer Network Defense (CND) community for effective identification, diagnosis and response.

(U) Discussion

- (U) NSA's primary point of contact for CND is the National Security Incident Response Center (NSIRC). NSIRC is a 24/7 activity that provides unique, tailored, all source, time critical, current and term technical and intelligence analysis, reporting and operations expertise on matters addressing the threat, detection, reaction, warning and response to intrusions into national security and critical infrastructure networks.

- (U) During an incident, NSA's NSIRC will coordinate with the Joint Task Force for Computer Network Defense at US Space Command, the DOD Computer Emergency Response Center, The FBI's National Infrastructure Protection Center and the GSA's Federal Computer Incident Response Center and the Intelligence Community.

(U) Way Ahead

- (U) The federal government's organizational framework is in place to manage a major cyber-attack but the procedural underpinnings and detailed operational roles are just now developing. If a major attack were to occur in the near future, close attention to managing the flow of information will be required within the community.

(U) CRYPTOMODERNIZATION

(U) The Department of Defense's (DoD's) vision[3] of a secure, seamless and collaborative information environment that will enable full situational awareness during military operations and achieve

[3] Joint Vision 2020

information dominance over any adversary cannot be achieved without modernizing its current information capabilities. A robust Information Assurance (IA) posture is an integral component of modernization and is essential to achieving the vision.

- ~~(C)~~ ***30 Years of Success*** - During the past 3 decades, the NSA has delivered a wide variety of COMSEC products to provide high-grade protection of critical C2 and Intel systems. These products are becoming increasingly hard to maintain and [redacted]

- (U//~~FOUO~~) ***From Links to Networks*** - In the past, we built point-to-point solutions, for voice, data and video systems. Today, Information Technology (IT) systems are moving to combine these into a common "network-centric" environment in which cryptographic solutions provide for a variety of Information Assurance (IA) services, such as non-repudiation, availability, integrity, etc.

- (U//~~FOUO~~) ***Interoperability Challenges*** - The U.S. military has increase interoperability requirements to support allied and coalition partners on a very dynamic basis. In the past we built US only equipment and then made decisions on release on a case-by-case basis. In today's environment, Information Assurance products must be built form day one with the goal of supporting allied/coalition operations.

- (U) ***Roadmap*** - A DoD-wide working group has been meeting since October with representation from across DoD to develop the crypto modernization roadmap which will lay out the strategy and provide an estimate of the cost to implement.

(b)(1)
(b)(3)-P.L. 86-36

~~COMINT~~
~~SECRET//X1~~

TRANSITION 2001

~~COMINT~~
~~SECRET//X1~~