~~SECRET//X1~~

NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE

TRANSITION 2001

December 2000

Derived From: NSA/CSS Manual 123
Date: 24 February 1998
Declassification: X1

~~SECRET//X1~~

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

22 December 2000

MEMORANDUM FOR OFFICE OF SECRETARY OF DEFENSE, EXECUTIVE SECRETARY

SUBJECT: Transition Books

Reference your 14 December 2000 memorandum from Colonel Marla I. Cribbs, USAF, Executive Secretary, subject as above.

The National Security Agency/Central Security Service provides the attached transition book for use by the DoD leadership of the next Administration. Information within this book includes: organization structure, key external relationships, budget profile, personnel resources and time-critical policy or management issues likely to require attention during the first six months of 2001.

In my capacity as Chief of the NSA/CSS 2001 Transition Team, I serve as the Agency's point of contact on all transition related matters and can be reached at 301-688-7357 or via e-mail at (b)(3):P.L. 86-36

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

Chief,
2001 Transition Team

This document may be downgraded to UNCLASSIFIED upon removal of enclosures.

~~SECRET//X1~~

NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE

2001 TRANSITION

DECEMBER 2000

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

~~SECRET//X1~~

(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

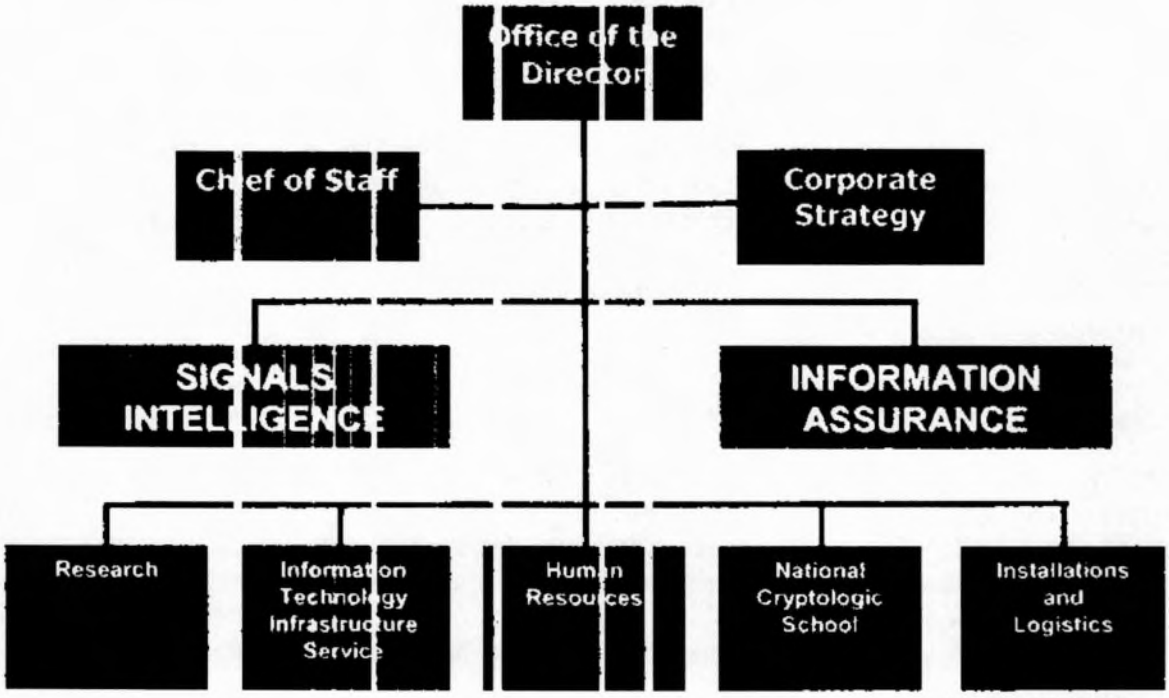
(U) INFORMATION SUPERIORITY FOR AMERICA AND ITS ALLIES

(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 workforce to meet SIGINT and Information Assurance mission challenges.

- (U) Build and sustain a diverse civilian, military (both active and reserve), and contractor workforce 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 with in 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.

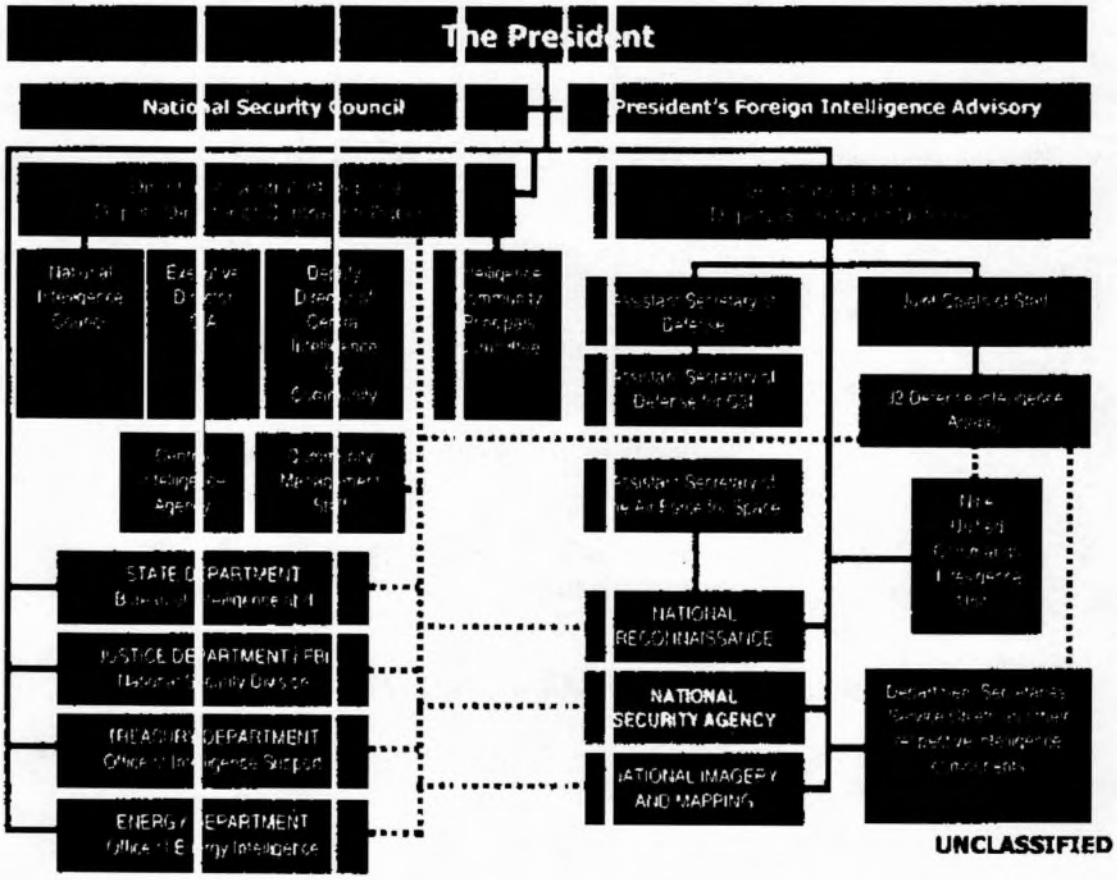
(U) MANAGEMENT

(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.



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

(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
- (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:

- 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] new 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.

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

(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.

(U) SSCI-HPSCI Conference

- ~~(S)~~ Authorized (b)(1); (b)(3):P.L. 86-36 positions for the CCP Program.
- ~~(S)~~ Authorized (b)(1); (b)(3):P.L. of 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 (b)(1); (b)(3):P.L. 86-36 for the CCP Program.
- (b)(1); (b)(3):P.L. 86-36
- (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 Plan.

~~(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 (b)(1); (b)(3):P.L. 86-36 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 (b)(1); (b)(3):P.L. 86-36 in FY02 and (b)(1); (b)(3):P.L. 86-36 across the FYDP (see the "Budget Issues" section below).

(U//~~FOUO~~) 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.

(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 (approximately another [redacted] (b)(3):P.L. 86-36 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] (b)(1); (b)(3):P.L. 86-36
Consolidated Cryptologic Program (CCP)	
Information Systems Security Program (ISSP)	
Defense Cryptologic Program (DCP)	[redacted] (b)(1); (b)(3):P.L. 86-36
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] (b)(1); (b)(3):P.L. 86-36						
Total NSA Billets							

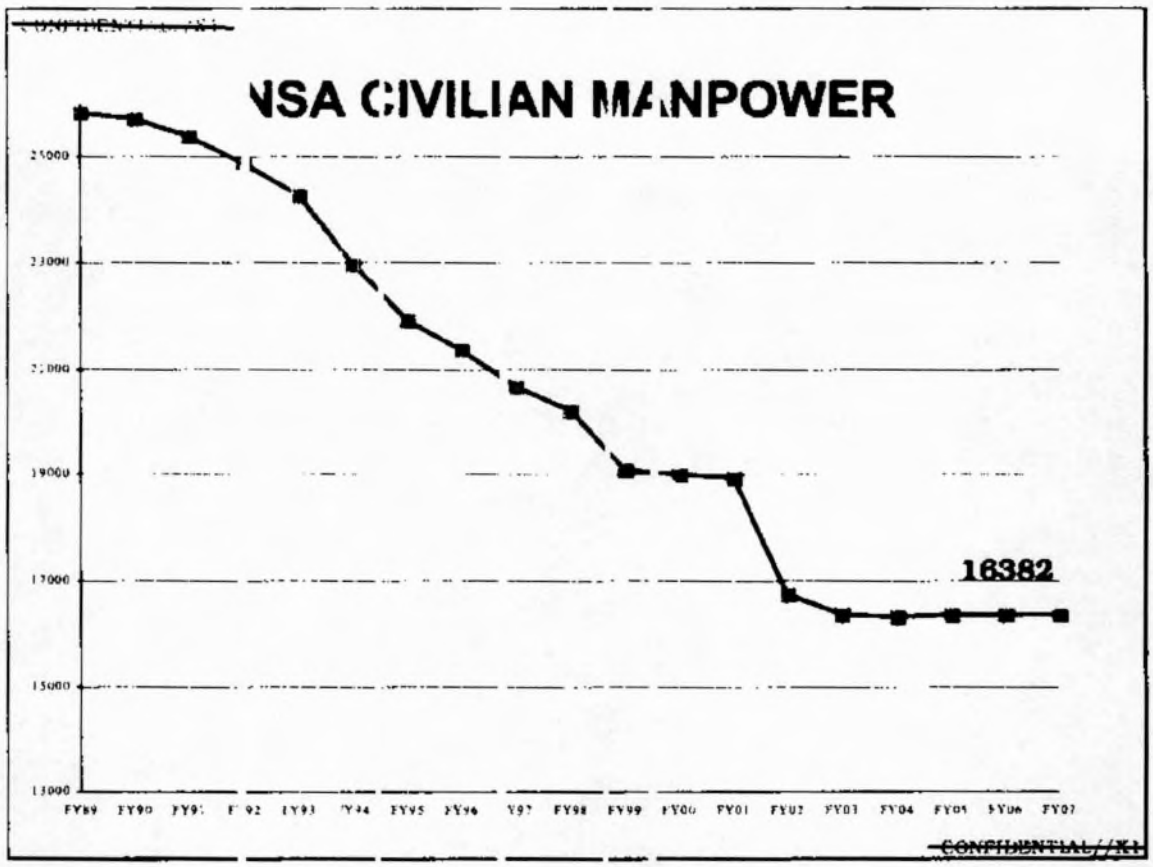
~~SECRET~~

(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.

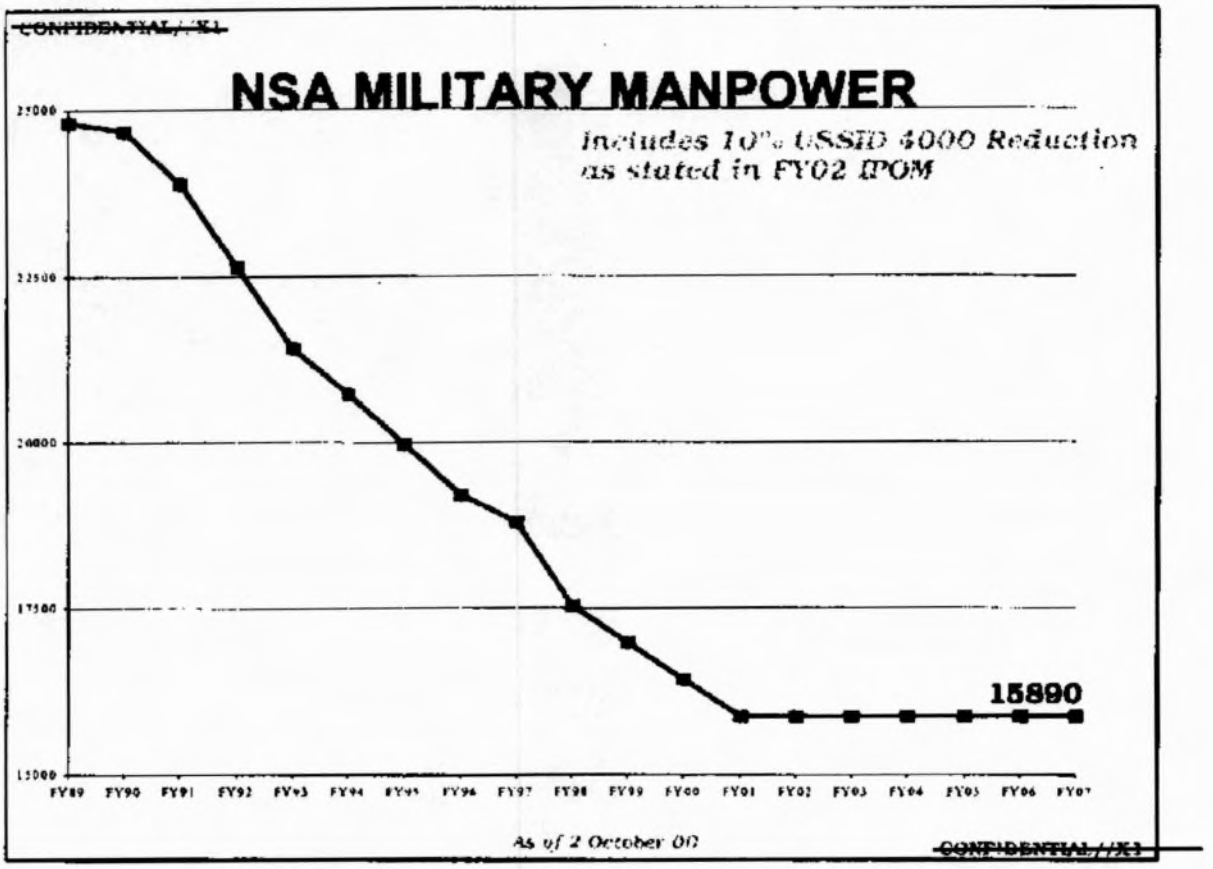
(b)(1); (b)(3):P.L. 86-36

(U) Figure 1


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

(U) Figure 2

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



(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, (b)(1); (b)(3):P.L. 86-36 Advanced capabilities that are needed today, particularly in the SIGINT analytic process, (b)(1); (b)(3):P.L. 86-36 as currently funded. (b)(1); (b)(3):P.L. 86-36 (b)(1); (b)(3):P.L. 86-36 A summary of NSA's specific overguidance requirements follows:

~~SECRET//X1~~

NSA OVERGUIDANCE *(in millions of dollars)*

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

[redacted]

	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

*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 3 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 Crypto modernization, Attack Sensing, Warning, & Response, and Information Assurance Solutions

TRANSITION 2001

(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 500 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)~~ The 16,000 military 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 16,155
  - ~~(C)~~ Part Time 974
- ~~(C)~~ Civilian Location
  - ~~(C)~~ Headquarters 14,145
  - ~~(C)~~ Deployed 2,010

- (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.

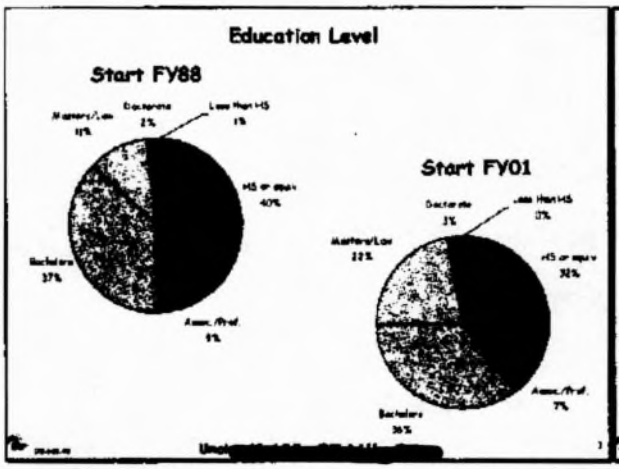
(U) MILITARY POPULATION (AS OF 19 DEC 00)

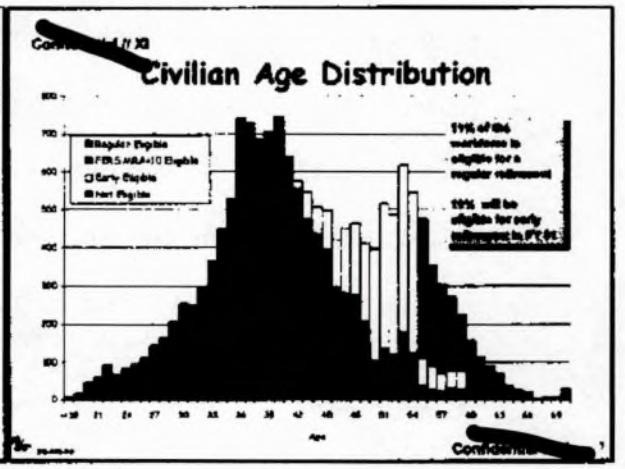
~~CONFIDENTIAL//X1~~

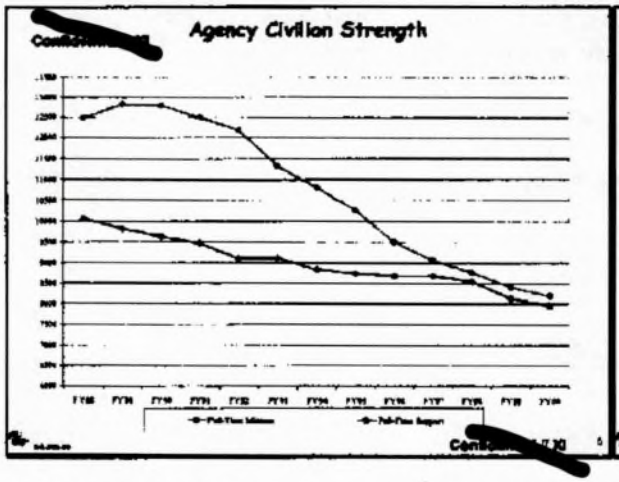
	AUTH	ASSIGN	%
ARMY	1067	831	77%
NAVY	955	867	91%
MARINES	163	150	92%
AIR FORCE	1825	1676	92%
TOTAL	4019	3524	88%

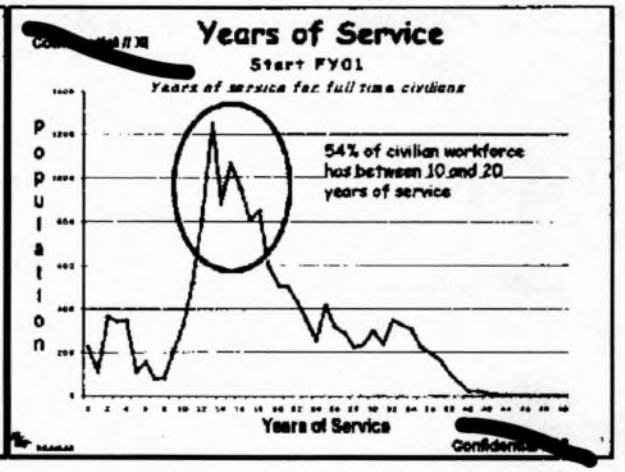
~~CONFIDENTIAL//X1~~

(U) Human resources summary slides follow.







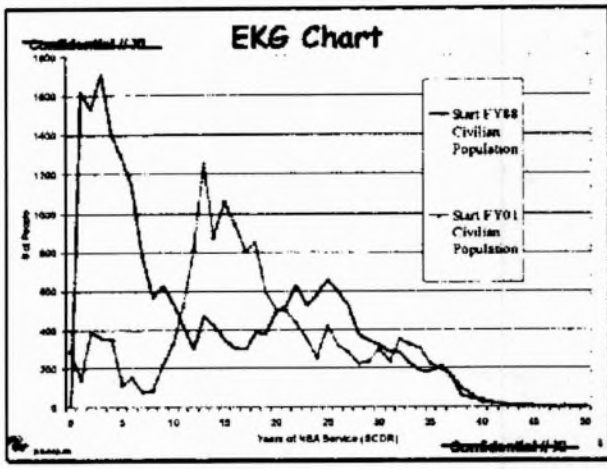


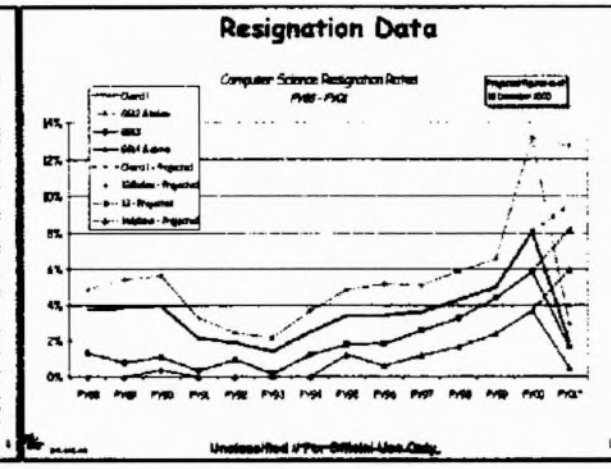
(U//~~FOUO~~) NSA has a highly educated workforce. The number of personnel with graduate and doctorate degrees has risen by 50% since FY88.

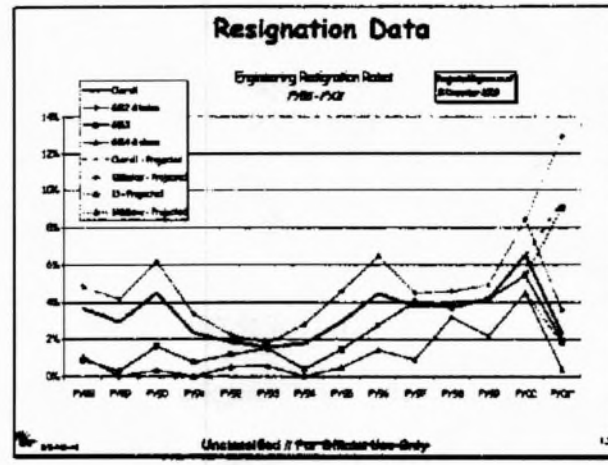
(U//~~FOUO~~) 11% of the workforce is eligible for regular retirement–19% will be eligible for early retirement in FY 01.

~~(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.

~~(S)~~ 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







(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

- ~~(C)~~ 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

TRANSITION 2001

(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 policy making 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. (b)(1); (b)(3):18 USC §798(a); (b)(3):50 USC § 403-1(i); (b)(3):P.L. 86-36

(b)(1); (b)(3):18 USC §798(a); (b)(3):50 USC § 403-1(i); (b)(3):P.L. 86-36

~~(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 stronger 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.

(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 30 decades, the NSA has delivered a wide variety of COMSEC products to provide high-grade protection of critical C2

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

- (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.

TRANSITION 2001

EXTERNAL TEAM REPORT

A MANAGEMENT REVIEW FOR THE DIRECTOR, NSA

OCTOBER 22, 1999

EXTERNAL TEAM REPORT

INTRODUCTION

Upon assuming command of the National Security Agency (NSA), Lieutenant General Michael V. Hayden, USAF, commissioned two management review teams, one comprised of NSA employees and another composed of five outside experts, named the External Review Team. This external the External Review Team began its work on August 9, 1999 with the stipulation that it would report to the Director, NSA within 60 days. General Hayden was briefed on The External Review Team's findings and recommendations on October 12. This document constitutes the final report of the External Review Team.

The five members of the External Review Team consider it a great honor to have been asked to participate in this important work. The NSA has long been one of America's preeminent governmental institutions whose successes, like those of its sister intelligence agencies, must often go unheralded. However, the need for secrecy, so critical to mission success, can also breed insularity, which is counterproductive to effective management.

This report aims at specific suggestions to the Director which will be actionable and which will produce rapid results. There have been a number of significant studies of NSA in selected areas over the past decade. Almost all have been done extremely well and offered good recommendations. But almost none of these recommendations have been implemented in a meaningful manner.

> *A major challenge facing NSA has been to understand why no action has occurred on the many previous excellent recommendations from multiple sources, and what can be done by General Hayden to ensure constructive change moving forward.*

We have been extremely impressed by the dedication and skill levels of NSA employees at all levels, but recognize from our own experiences in business and in government that individual actions are usually not enough to initiate corporate-wide change. It took new Chief Executive Officers at IBM and AT&T to re-energize those previously distinguished businesses. It is our expectation that General Hayden will fulfill that same role at NSA.

The majority of senior level employees with whom we spoke believe that this entire series of managerial issues has come to the fore as a result of the ongoing reduction in resources, i.e. budget cuts, combined with an expanding demand for its excellent work. NSA funding has been reduced dramatically over the last several years. Unanimously, the

External Review Team believes that the managerial issues would be no different should prior funding levels be restored. Money alone is not the answer.

The NSA mission is a cornerstone of many other aspects of American intelligence work. NSA is too critical to the wellbeing of our society today, and tomorrow, for the Agency to be allowed to function in a sub-optimal fashion. The House Permanent Select Committee on Intelligence has, correctly in our opinion, directed NSA to "change your culture and method of operations." The only question is how this might best be accomplished.

TASKING AND METHODOLOGY

The External Review Team was specifically tasked to review prior studies and reports (including the recent Clapper Brief) and evaluate Congressional language as it relates to NSA reform. We were asked to assess NSA's personnel culture, organization and processes, to document our findings and to present detailed recommendations for improvement. The Director placed no constraints on the scope of this study. However, Congress, the Secretary of Defense and the DCI expect "significant change" in how the Agency does business.

Our methodology was to research governing and historical documents and to review prior studies and investigations. We interviewed over one hundred people (both within and without NSA), including Agency seniors, mid-level and working staff, Congressional staffers and various NSA management teams including the Senior Agency Leadership Team [SALT]). The External Review Team met weekly to receive corporate briefings, hold meetings with senior level personnel and update the Director on the study's progress. After collecting and analyzing all the data, The External Review Team formally briefed General Hayden and prepared this report.

FINDINGS

We determined many good features of the Agency throughout the report. We agreed that at least the following aspects of the Agency were positive:

- Stakeholders consider the Agency to be critical to national security
- The Agency has certain world-class competencies
- The leadership and staff care deeply about their institution
- The institution cares about its people
- The Agency has responded well in the past to national crisis.

However, we enumerated many issues throughout this report. We agreed there are at least ten significant areas of concern:

- Poorly communicated mission and lack of vision

- Broken decision making process which is demonstrated by a lack of accountability and empowerment
- Poor financial management
- Broken personnel system
- Broken requirements process; timeliness, responsiveness, constraints, and other key parameters are not being properly considered
- Inadequate business management, program management, and system engineering
- Poor stakeholder relations, particularly with Congress
- Inward looking culture
- Risk of technology obsolescence, gap with commercial practice
- Dissatisfaction with senior leadership (even within senior leadership).

The most serious issues are leadership, accountability, and empowerment, as evidenced by great dissatisfaction with decision making within the Agency.

New Enterprise Team (NETeam) Recommendations

1 October 1999

The Director's Work Plan for Change

The overall classification of this document is ~~SECRET~~. It has not yet been portion marked.

Your Work Plan to Reach NSA II

Near-term - 30 days: Regain confidence of stakeholders about our ability to chart course for future

Mid-term - 180 days: Synchronize with stakeholders; institutionalize governance practices; make leadership a central attribute

Long term - 2 years: Begin cultural, technological and business focus shift to the 21st Century (NSA II)

Decision-making

- Replace SALT structure with new executive leadership team
- Define/document governance process
- Ensure that ELT has the data it needs; develop an MIS

Leadership

- Establish leadership standards
- Devote resources to change management
- Reinvigorate programs to groom leaders

Strategic alignment

- Create strategic business plans; implement plans; align budget and people with plans
- Complete transformation to NSA II

Resource allocation

- Hire financial management officer; Fix resource management
- Get systems development under control
- Create SIGINT modernization organization

Relationships with customers, partners, stakeholders

- Develop customer/partner/stakeholder strategies; Implement strategies

Workforce

- Revise pay system
- Develop workforce skills

options. But our unanimous conclusion is that restructuring the Agency is secondary to fixing the fundamental problems: lack of leadership, lack of governance, and lack of strategic alignment. Fix those, and you'll be well on your way to turning the Agency around and leading us into the 21st Century.

On the next page is an illustration of our key recommendations in time-line format. The body and appendix contain additional recommendations.

Six Quick Hits to Show We're Serious

We have recommended that you undertake a number of initiatives aimed at fixing the basics of the NSA institution. There are also a number of practices and processes that should be stopped immediately. Our selection of the items below is based on focusing our resources in alignment with NSA's corporate strategy and business plan by stopping, for the short term, activities that drain energy, labor and dollars from serving our core missions until that alignment can be accomplished.

1. Abolish all senior personnel boards and make senior promotions and job placement the job of the senior leadership team. You currently have approximately 45 seniors and a number of dedicated support personnel tied up for significant periods of time in senior personnel activities. You have no strategy or plan for senior personnel development and succession planning. Develop the plan and make implementation the job of senior leadership. Allow only one senior personnel board to be formed. Do not allow the subordinate boards to be "regrown".

2. Scrub completely the list of "senior positions" and stop selecting people to fill them based only on rank. If the position is needed, then we should be most concerned about putting the right person in the job, vice putting a senior in a job because of tradition. Put the best qualified person in these jobs, even if they are "junior".

3. Abolish Agency level promotion boards and return promotion authority to the Key Component level. The existing promotion process consumes almost all the time of approximately 30 people (seniors and our highest potential 15's, and dedicated support personnel). The "value-added" of this expenditure of time is questionable, at best.

4. Within one week each Key Component should be directed to eliminate all working groups and committees where a single individual could make decisions, and also eliminate those that are not critical to performing the SIGINT and INFOSEC missions. NSA has too many working groups and committees. Senior leaders (not committees) need to make the hard decisions that need to be made. The workforce needs to apply their talents to the core mission, and not spend time commuting to and attending meetings.

5. Stop the ongoing review of the NSA leadership curriculum until the leadership competencies we require in our institution are defined and aligned with NSA's corporate strategy and business plan. NSA has never embraced leadership and management as core competencies—they are not designated NSA career fields, nor is even minimum training required to occupy leadership or management positions. While we applaud the desire to review the curriculum, we argue that NSA does not have the skills or background necessary for success. Moreover, NSA does not need to develop its own curriculum. We recommend that NSA examine the courses available in private industry and in the government, and adopt/adapt their use rather than developing all homegrown management and leadership training.

6. Stop initiation of any new programs or initiatives (other than organizational consolidations related to support or corporate governance processes) until business planning is complete, and budget and labor appropriately aligned to support it.

Mid-term (6 months): Align ourselves to the corporate strategy—move toward NSA II

As soon as the plans are completed, you and the ELT must ruthlessly and relentlessly drive their implementation at all levels of the Agency. Again, this is your job. It's up to leadership to develop the framework for change—and to be the agents of change. In fact, given the sweeping changes that lie ahead, we recommend you make change itself a strategic goal.

Specific mid-term tasks:

It's up to leadership to develop the framework for change—and to be the agents of change.

- Align the budget and workforce with the corporate strategy. You must get systems development under control, stop duplicative efforts, and ensure that the entire workforce is marching to the beat of the business plan.
- Implement a corporate strategy for dealing with customers, partners and stakeholders. You must ensure that we speak to our external constituents with a single voice.
- Create a leadership pipeline. You must set up programs to identify and groom tomorrow's leaders—so we'll never again be in a position where we lack the leadership to implement change.
- Begin the transformation to NSA II, our term for the next-generation NSA. Although this a long-term effort, we believe you must start right away by creating a program management organization with the authority and responsibility for all SIGINT modernization efforts.

None of this will be possible without the workforce; therefore, we urge you to take immediate steps to ensure you have the necessary skill mix—and the flexibility to modify it as needed. Accomplishing this will require a major overhaul of the current HR system, to include aligning our hiring with the corporate strategy, reforming our pay system, and increasing our use of outside expertise. It's a long-term task, but it must begin soon. Key to success will be expanding the definition of stakeholder to include the workforce as a full-fledged member—make your workforce a full partner in developing HR solutions.

Long-term (2 years): Complete the transformation to NSA II

What's left for the long-term is to complete the transformation of NSA into NSA II. Restructuring is probably inevitable, and we offer several

Executive Summary

After 60 days of study, it boils down to this: get back to basics, put NSA on a solid business footing, and do it now.

We've identified six issues that demand your attention:

- Our decision-making process is ineffective.
- We lack effective leadership.
- We are not aligned to a corporate strategy.
- We focus more on our own "tradecraft" than on our customers, partners, and stakeholders
- Our resource management is out of control.
- Our work force is not prepared for the future.

Near-term (30 days): Tackle leadership and decision-making

To tackle the issues, you must start at the top, with leadership and governance. First, fix the SALT—it's ineffective. Streamline it into a powerful executive leadership team (ELT) with fewer members, tighter procedures, and a mission focus. Hire a financial management officer (FMO) with the business savvy to put our house in order and give him or her the authority to manage our finances. And provide the ELT with a clear understanding of the rules of the road—a well-defined governance process. The DICM should define the process; it will be up to you to enforce it. You must also immediately establish standards against which the executive leadership team, and indeed all Agency leaders, will be judged. These are the basic tools—you must have them in your tool-kit before you can do anything else.

To tackle the issues, you must start at the top, with leadership and governance. First, fix the SALT—it's ineffective.

Now the real work begins. You and your new ELT must develop a strategic plan and a business plan. The plans must begin and end with the customer—not our "tradecraft"—and they must be clear enough and specific enough to chart our course. Please do not delegate this to a staff; we strongly believe it's a leadership responsibility.

Order Code RL30740

CRS Report for Congress

Received through the CRS Web

The National Security Agency: Issues for Congress

November 17, 2000

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

The National Security Agency: Issues for Congress

Summary

The National Security Agency (NSA) one of the largest components of the U.S. Intelligence Community, has reached a major watershed in its history. Responsible for obtaining intelligence from international communications, NSA's efforts are being challenged by the multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states.

NSA's efforts to adjust to the changing geopolitical and technological environment have been strongly encouraged by Congress and reflect a major shift in congressional oversight of the Agency. Although Congress has always approved funding for NSA, for decades routine oversight was limited to a few Members and staff. In the 1970s, congressional investigations of intelligence agencies resulted in greater public attention to NSA and criticism of activities that infringed on the civil liberties of U.S. persons. Subsequently, both the Senate and the House of Representatives established intelligence oversight committees that have closely monitored NSA's operations. The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 to regulate collection by foreign intelligence agencies of the communications of U.S. persons. The end of the Cold War, the expansion of low-cost encryption and the explosion of communications systems led Congress to take a more public profile in overseeing the large and secretive Agency.

Reacting in large measure to congressional concerns, NSA launched two separate management reviews, one by outside experts, the other by longtime Agency officials. Both made strong criticisms of Agency personnel policies, an outmoded organizational structure, and an unwillingness to utilize civilian practices that more effective than those available in-house. The current NSA Director, Lt. General Michael V. Hayden, USAF, has used these analyses to launch a series of major initiatives designed to improve NSA's operations, to attract and reward more qualified people from outside industry, and is developing a major contract for outside support of its non-sensitive Information Technology (IT) functions.

A major renewal effort is underway, but observers believe many challenges lie ahead that will require congressional oversight. Many of the reforms in personnel policies recommended are difficult to implement in a government organization, especially in an extremely tight market for technical specialists. The technical complexities of dealing with widespread and sophisticated encryption as well as the proliferation of communications devices remain to be resolved. NSA is, along with other intelligence agencies, not well-positioned to analyze developments among the assortment of terrorist groups and narcotics smugglers around the world that can seriously affect U.S. interests. NSA has also come under heated criticism in the European Parliament for allegedly collecting, in cooperation with the British, commercial intelligence to benefit U.S. corporations.

Contents

The National Security Agency: Issues for Congress

Introduction

The National Security Agency (NSA), one of the largest components of the U.S. Intelligence Community, has reached a major watershed in its history. Responsible for obtaining intelligence from international communications,[1] NSA's efforts are being challenged by the multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states.

NSA was established in 1952 as a highly compartmented secret codebreaking effort undertaken by a handful of military officers and civilians, but the Agency has gradually become an acknowledged government agency responsible for signals intelligence (sigint). This evolution has been in significant measure a result of congressional initiatives. Congress provided the statutory framework for NSA and its activities. Laws have been enacted that carefully prescribe the limits of NSA's electronic surveillance of U.S. persons. Congress has been increasingly inclined to take public notice of problems at NSA and is supporting reforms that are designed to make NSA more effective in current technological and geopolitical environments.

The challenges facing NSA are formidable: a difficult operational environment as well as limitations on spending levels for intelligence call into question the future capabilities of NSA. Public interest in NSA has been heightened in recent months by some members of the European Parliament who allege that the United States and a few other countries are cooperatively engaged in systematic electronic eavesdropping in order to promote the commercial interests of U.S. corporations. This Report will

---

[1] A primary responsibility of NSA is the collection and analysis of signals intelligence a function that has been described by Director of Central Intelligence George Tenet as "one of the pillars of US intelligence. Along with our other intelligence collection activities, we rely on SIGINT to collect information about the capabilities and intentions of foreign powers, organizations and persons to support the foreign policy and other national interests fo the United States. SIGINT is critical to monitoring terrorist activities, arms control compliance, narcotics trafficking, and the development of chemical and biological weapons and weapons of mass destruction." Statement by Director of Central Intelligence George J. Tenet before the House Permanent Select Committee on Intelligence, April 12, 2000. NSA is also responsible for protecting information systems security of U.S. Government agencies. This is an increasingly important NSA mission that includes the preparation of codes and encoding devices, but the focus of this report will be on the more controversial intelligence collection and analysis mission.

attempt to provide an unclassified description of NSA's evolution, the technical and operational environment that now exists, and indicate some issues that the executive branch and Congress will be facing in coming years.

An unmistakable change affecting NSA has been the openness with which its policies and problems are now discussed both by the Agency's leadership and by congressional oversight committees. Until very recently NSA was the most secretive intelligence agency, more shielded from public scrutiny than the Central Intelligence Agency (CIA). Only the most elliptical references were made in public to the sigint mission, and at one time, NSA employees identified themselves only as working for the Defense Department. In the past few years, however, senior intelligence officials frequently describe NSA's problems and reports accompanying intelligence legislation include extensive commentary on the challenges facing NSA and the approaches encouraged by Congress. These changes were made possible by the absence of a superpower competitor capable of exploiting any inadvertent security slip and by the need to justify intelligence spending at a time when international climate is apparently more benign. These factors removed inhibitions against NSA "going public" and, at the same time, created a political environment that would require public understanding of NSA's mission if the Agency could continue to obtain the funding necessary to update its operations.

Roles and Missions: The Growing Influence of Congress

For decades Congress was content to consider the signals intelligence effort and the organization of NSA primarily as the responsibility of the executive branch. For a quarter century after the end of the Second World War, NSA and the nation's other intelligence agencies undertook their activities with little publicity and with congressional interest limited to a handful of members of armed services and appropriations committees. The intelligence investigations of the 1970s, however, led to well-publicized hearings that placed many secrets, including those of NSA, on the public record. Of greater enduring significance was the establishment of select intelligence committees in both the House of Representatives and the Senate. These committees were granted the authority to conduct oversight over the intelligence activities of the Federal Government, including NSA. They became, along with the appropriations committees, the points of contact between the intelligence agencies and Congress. As a result of the extreme sensitivity of much intelligence information, the two intelligence committees came to act essentially as surrogates for the Congress and the public in regard to intelligence agencies. Until the mid-1990s much of interest of the committees, as reflected in report language and public hearings, centered on the CIA and especially its operations directorate. Sigint activities were undoubtedly matters of congressional concern, but they were very rarely the focus of public attention.[2]

In recent years, with the end of the Cold War the two intelligence committees have had much more intensive concern with NSA as reflected in more detailed report language on NSA's activities. The extent of oversight is reflected by comments in

---

[2] For additional information on congressional oversight of NSA, see Appendix A.

the report on the FY2000 Intelligence Authorization bill (H.R. 1555) by the House intelligence committee:

> In the last two Congresses, the committee has been direct in its identification of process and management problems that require attention. The committee believes that NSA management has not yet stepped up to the line. There have been some efforts at reform, but there are still several areas where change is not only needed but is critical for NSA's future.[3]

Congress has taken a more open interest in NSA at a time when the Agency's roles and missions are facing significant reformulation. Congress has provided guidance for NSA's future direction and has made budgetary allocations based on its sense of appropriate goals, personnel policies and organizational structure. Most observers believe, moreover, that given the fluid state of international affairs and information technologies, that further congressional attention is likely as NSA changes to adapt to its new environment.

Changing Technologies

The primary targets of electronic surveillance during the Cold War were the communications of hostile military organizations and governments. Most of such communications were encrypted; in many cases this message traffic could be read only sporadically, if at all (although useful information can often be obtained without actually reading the actual messages). Some communications were carried on land lines that could be intercepted only if they could be physically tapped, inevitably a difficult undertaking. It was, nonetheless, the government and military circuits that provided the most important intelligence of military capabilities, hostile intentions, and diplomatic maneuvers that could place this nation's security at risk. Civilian communications–telegraphs, telephones, facsimile devices, etc.–were usually unencrypted and often sources of valuable information, albeit of secondary priority.

In the past decade, two important trends have combined to change the nature of electronic surveillance efforts. The end of the Cold War meant policymakers and military officials had a wider range of countries that they were concerned with and placed much greater emphasis on "non-state actors"–terrorist groups and narcotics smuggling organizations that have come to be seen as genuine national security threats. These links are not necessarily easy targets given the great expansion in international telephone service that has grown by approximately 18% annually since 1992. Intelligence agencies are faced with profound "needle- in-a-haystack" challenges; it being estimated that in 1997 there were some 82 billion minutes of telephone service worldwide.[4]

---

[3] U.S. Congress, 106th Congress, 1st session, House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2000*, H.Rept. 106-130, Part 1, May 7, 1999, p. 12.

[4] Linda Blake and Jim Landes, *Trends in the U.S. International Telecommunications Industry* (Washington: Federal Communications Commission, 1999), tables 7,9.

The technologies used in civilian communications circuits have also changed: in the past decade reliance on microwave transmissions (which can be intercepted with relative efficiency) has been increasingly displaced by fiber optic cables.[5] Fiber optics can carry far more circuits with greater clarity and through longer distances and provides the greater bandwidth necessary for transmitting the enormous quantities of data commonplace in the Internet age. Inevitably, fiber optic transmission present major challenges to electronic surveillance efforts as their contents cannot be readily intercepted, at least without direct access to the cables themselves. The widespread use of fiber optics may also affect requirements for expensive sigint satellites since transmissions over fiber optic cables cannot be intercepted from space-based platforms.[6]

In addition to the widespread use of fiber optic cable, civilian communications have been marked by increased access to high-quality encryption systems formerly available only to governments and militaries. Some systems are available at no cost on the Internet and others can be obtained commercially at minimal expense. This has led to an extensive debate in the United States about the need for export controls on sophisticated encryption systems. Although it is universally acknowledged that commercial encryption systems available throughout the world present major challenges to intelligence (and law enforcement) agencies, U.S. intelligence officials have argued that permitting export of high-quality U.S. systems with associated systems support would greatly extend the capabilities of other governments and hostile groups to protect their communications. After extensive discussions within the executive branch and Congress, steps have been taken to loosen, but not remove, U.S. restrictions on encryption exports.[7] NSA officials were active in criticizing unrestricted encryption exports and observers suggest that these views, which were shared by many in Congress especially within the intelligence and armed services committees, may have fueled press criticism of NSA.

Changing threats, coupled with the evolving global technological environment, have undoubtedly made NSA's tasks far more difficult. The proliferation of communications throughout the world and the spread of encryption may make electronic surveillance almost impossible. Much equipment acquired for Cold War missions is not effective against new targets. In some cases, NSA must resort to analyses of traffic patterns–who is communicating with whom, when, and how often–to provide information that may not be obtainable through breaking of codes and reading of plaintext.

A major shortcoming was revealed in January 2000 when a software anomaly in the communications infrastructure curtailed NSA's operations for some 72 hours. An

---

[5] See Ivan Amato, "Fiber Optics: Communicating at Light Speed," *Washington Post*, November 10, 1999, p. H1; Lee Bruno, "Broadband: To Infinity and Beyond," *Red Herring*, February 2000, p. 170.

[6] See Jeremy Singer, "Sophisticated Fiber Optics Also Problematic for NSA," *Defense News*, June 12, 2000.

[7] See Richard M. Nunno, *Encryption Technology: Congressional Issues*, CRS Issue Brief IB96039; Richard A. Best, Jr. and Keith G. Tidball, *The Encryption Debate: Intelligence Aspects*, CRS Report 98-905, November 4, 1998.

intensive and expensive effort was required to restore operations. A subsequent assessment found that the fundamental problem was not technical, but doctrinal and organizational.[8]

Personnel Matters

NSA has employed many highly gifted scientists, engineers, and mathematicians. However, shifting geopolitical concerns and budget reductions required in the early 1990's led to early retirements and fewer newly hired employees. During the same period, the Agency was also required to move towards a personnel structure more closely reflective of national demographics. Simultaneously, a revolution in communications and information technologies was launched in many small, start-up firms whose culture and salary and personnel benefit levels were radically different from those of government agencies. As the extent of these problems became apparent, Congress has provided guidance in several areas.

Diversity and Equal Opportunity Issues

At least since the enactment of the National Security Agency Act of 1959 NSA's personnel policies have been the subject of congressional interest. That Act in essence established a separate personnel system for NSA. By the mid-1980s the House Intelligence Committee became concerned with the relatively small numbers of African-Americans, Hispanics, and women within the NSA workforce. (In 1993, blacks constituted 9% of the total number of NSA employees whereas the national labor force percentage was just over 10; the NSA Hispanic percentage was 1.2, whereas the national average was just over 8; for Asian Americans, the national figure was 2.9, at NSA it was 0.9.)[9] One congressional initiative included provisions in the FY1987 Intelligence Authorization Act (P.L. 99-569) amending the National Security Agency Act to establish an undergraduate training program to facilitate the recruitment of minority high school students with skills in mathematics, computer sciences, engineering and foreign languages. Recruitment efforts were made in colleges with higher concentrations of Hispanic students and efforts were made to ensure equal consideration in promotions. By 1996, NSA had made measurable increases in minority and female representation in the general workforce and in

---

[8] See Walter Pincus, "NSA System Crash Raises Hill Worries," *Washington Post*, February 2, 2000, p. 19. Michael V. Hayden, "Background on NSA: History, Oversight, Relevance for Today," *Defense Intelligence Journal*, Summer 2000, p. 31. During this period the British reportedly helped to supply data that NSA could not obtain directly; see Ben MacIntyre, "UK Spied for US as Computer Bug Hit," *Times* (London), April 27, 2000.

[9] Statement of Vice Admiral J.M. McConnell, USN, Director, National Security Agency/Chief Central Security Service in U.S. Congress, 103rd Congress, 1st session, House of Representatives, Permanent Select Committee on Intelligence, *Central Intelligence Agency, Defense Intelligence Agency and National Security Agency: Minority Hire, Retentions and Promotions*, Hearing, October 28, 1993, p. 27.

leadership positions.[10] These initiatives were not welcomed by all NSA personnel, with some officials expressing concerns that others would receive preference at their own expense.[11] Since the mid-1990s public congressional hearings and published committee reports have not given extensive discussion to diversity issues. Although efforts continue to increase the diversity of NSA's workforce, other personnel issues have complicated hiring and promotion policies.

Changing Personnel Requirements

Since the end of the Cold War, the nature of sigint targets has changed; the sheer quantity of communications has dramatically risen and sophisticated encryption systems are increasingly available throughout the world. These changes in targets and technologies have required a substantially different NSA workforce. Long staffed by civil servants and military personnel who made their whole careers in cryptologic specialities; NSA officials must now be able to shift rapidly among disparate sigint efforts and varying targets. Different skill mixes are required at NSA at a time when technical specialists in communications, computer services, and encryption systems are in high demand throughout the economy. Observers believe that entry- and mid-level government salaries are not equal to opportunities currently available in an especially dynamic sector of the economy; furthermore, workers in technical fields often shift jobs in short periods and it may not be possible to retain them solely on the basis of the career benefits of federal service.[12]

As has been the case with other intelligence agencies, staffing levels at NSA have been reduced during the past decade. Many analysts and others who spent their careers focusing on Soviet and Warsaw Pact issues no longer directly relevant to U.S. security concerns have retired or moved into new specialities. Some media observers suggest, however, that NSA continues to be burdened by an "old guard" of Cold War-era careerists whose talents are not precisely suitable to emerging missions. Although such charges are difficult to document (and may only reflect bureaucratic politics), it is generally acknowledged that NSA will have to adopt an altered personnel structure. FY2001 Intelligence Authorization legislation (passed by both houses, but vetoed by the President because of concerns not directly related to NSA) would provide authority for NSA to offer early retirement and voluntary separation

---

[10] U.S. Congress, 104th Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Human Resources and Diversity*, Hearing, September 20, 1996, pp. 28-29.

[11] U.S. Congress, 103d Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Hiring, Promotion, Retention and Overall Representation of Minorities, Women and Disabled Persons within the Intelligence Community*, Hearing, September 20, 1994, pp. 124-125.

[12] In November 2000 the Office of Personnel Management announced that it was establishing higher rates of basic pay for entry- and mid-level information technology (IT) workers throughout the Federal Government, with net pay increases ranging from 7 to 33%. The IT categories involved include a significant number of positions at NSA. NSA is also preparing to implement a new compensation structure that will use variable pay to recognize and reward achievement. See "NSA Chief Pushes Ahead with Overhaul of Agency's Culture, Operations," *Defense Information and Electronics Report*, October 20, 2000, p. 5.

pay to employees with 20 or 25 years of service (depending on age). This provision was inserted to provide the NSA Director with the opportunity to institute personnel changes that are considered necessary and reflects the intelligence committees view that "the situation at NSA is unique, not only in the enormity of the task of modernization, but also in the direct impact on national security should NSA modernization fail."[13]

One approach that has been adopted is to increase reliance on contracting out personnel services although security considerations can complicate the use of non-career personnel.[14] In some cases it has been possible to acquire the services of some retired NSA officials who are able to receive the relevant clearances with little delay. In other situations NSA is able to compartmentalize some activities and make use of specialists who do not need access to sensitive information. Some observers warn, however, that contract personnel will tend not to be as committed to the Agency's missions, and may work subsequently for non-government concerns with an increased possibility of unauthorized sharing of classified information.

Charting NSA's Future Direction

In recent years, congressional oversight committees have become concerned about the effect of the changed international threat environment and new technologies on NSA's future effectiveness. The requirement to replace aging satellite systems in particular have placed pressures on intelligence spending across the board; the size and extent of NSA's budget inevitably mean that it would be subject to close scrutiny. Thus, in 1997 the Senate Select Committee on Intelligence established a Technical Advisory Group (TAG) to review the U.S. sigint effort along with other technical challenges facing the Intelligence Community. The TAG was composed of leading U.S. scientists and experts in technology and intelligence and has made two classified reports on NSA's capabilities. According to the Senate Committee, the TAG identified serious deficiencies; "as resources have been reduced, the NSA systematically has sacrificed infrastructure modernization in order to meet day-to-day intelligence requirements. Consequently, the organization begins the 21st Century lacking the technological infrastructure and human resources needed even to maintain the status quo, much less meet emerging challenges."[15] One media account indicates that the TAG's conclusions were highly critical: "'We told them that unless you totally change your intelligence-collection systems you will go deaf,' one involved official [stated]. 'You've got ten years.'" According to the account, the Group

---

[13] U.S. Congress, 106th Congress, 2d session, Committee of Conference, *Intelligence Authorization Act for Fiscal Year 2001*, H.Rept. 106-969, October 11, 2000, p. 46.

[14] George Cahlink, "NSA May Outsource 5,000 High Technology Jobs," *Defense News*, June 12, 2000, p. 4

[15] U.S. Congress, 106th Congress, 2d session, Senate, Select Committee on Intelligence, *Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System*, S.Rept. 106-279, May 4, 2000, p. 6.

"urged that the agency immediately begin a major reorganization, and start planning for the recruitment of several thousand skilled computer scientists."[16]

According to the Senate report, the TAG also recommended new business procedures and additional resources. The report indicated that the FY2001 authorization bill would likely reflect TAG recommendations, with resources being shifted to long-term infrastructure modernization at the expense of some short-term collection.[17]

The House Permanent Select Committee on Intelligence also reached the conclusion in 1998 that "very large changes in the National Security Agency's culture and method of operations need to take place."[18] The Committee indicated its approach:

> First, the committee is funding and mandating external management reviews. Second, the committee is attempting to infuse fresh thought, needed expertise (especially in systems engineering), and greater fairness by insisting that significant portions of certain categories be contracted out and that outside proposals and expertise be solicited, notably in systems engineering, advanced research and development, and in development activities.... Third, fences have been placed on portions of the budget, with the prospect that a considerable amount of money could be reprogrammed for other [Intelligence Community] needs if NSA does not develop detailed strategic and business planning.[19]

The House committee envisioned "a far more radical revision of the budget process than presently contemplated." Emphasis would be placed on "a new culture in which all team together on a new architecture."

Director Hayden's Initiatives

Aware of the challenges facing the Nation's sigint effort and responsive to congressional concerns, the senior leadership of NSA has been moving to make drastic changes in NSA's operations and organization. Upon becoming NSA's director in March 1999 Air Force Lt. General V. Michael Hayden assigned a number of mid-level NSA officials to review the Agency's organizational structure. Known as the New Enterprise Team, the group recommended a new executive leadership team, the development of strategic business plans, the acquisition of agency wide management information systems, and hiring a financial management officer. A

---

[16] Seymour M. Hersh, "The Intelligence Gap," *New Yorker*, December 6, 1999, pp. 62, 64.

[17] Additional background on NSA's managerial challenges is provided in "NSA Overhauls Corporate Structure in Effort to Improve Operations," *Inside the Air Force*, June 23, 2000.

[18] U.S. Congress, 105th Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 1999*, H. Rept. 105-508, May 5, 1998, pp. 9-10.

[19] Ibid., p. 10.

separate report by a smaller group of outside experts with experience in the telecommunications industry made similar recommendations.[20]

The two sets of recommendations reflected a consensus by these advisory groups (and by congressional overseers) that NSA requires more centralized management, that separate divisions that had long enjoyed functional independence need greater coordination to reduce duplicative functions, and that there needs to be a strategic vision of how the Agency is to adapt to changed geopolitical and technological environments. Both reports reflected confidence in the importance of NSA's missions, but both were highly critical of NSA's management and personnel structures. The outside experts concluded: "The most serious issues are leadership, accountability, and empowerment, as evidenced by great dissatisfaction with decision making within the Agency."[21] The NSA officials noted the Agency's fundamental problems: "lack of governance, lack of leadership, and lack of strategic alignment." Although some specific criticisms reflect the inherent limitations of government agencies in comparison with the civilian telecommunications industry, NSA was urged to take special steps to hold middle managers responsible for personnel decisions. Although NSA has traditionally hired recent college graduates and retained them until retirement, changes in technology, in the international environment, as well as disparities in government and civilian salaries, imply that in the future there may be fixed-term positions and upgraded salary levels for some critical technical specialists.

NSA was also urged to move away from its traditional preference for performing all functions in-house rather than to look for creative ways to find civilian contractors not just as sources of manpower but as "solution providers," and to make hard choices over priorities rather than to make across-the-board budgetary reductions. The outside team of experts urged NSA not only to take advantage of the potential advantages of outsourcing but also to bring in mid- and upper-level managers from successful businesses.

In November 1999, Hayden launched "100 Days of Change"–another series of managerial initiatives responsive to the recommendations of these groups. He subsequently summarized NSA's challenges: "maintaining a strong infrastructure of people and facilities in a time of constrained budgets; accurately forecasting technology trends in the face of an explosion of information systems; and reacting agilely to new technological innovations."[22]

With congressional support Hayden has brought in industry experts from civilian firms to develop a comprehensive business plan for the Agency that will enable it to perform in a transformed global information technology arena. An initial step was the

---

[20] Bob Brewin, Daniel Verton, and William Matthews, "NSA Playing IT Catch-Up," *Federal Computer Week*, December 6, 1999, p. 1. The reports by NSA officials, New Enterprise Team, *The Director's Work Plan for Change*, October 1, 1990, and the External Team Report, October 22, 1999, were subsequently made available on NSA's Web site [http://www.nsa.gov].

[21] External Team Report, October 22, 1999, p. 4.

[22] NSA Press Release, 7 January 2000 *Director of National Security Agency Welcomes Ms. Beverly Wright, Chief Financial Manager.*

appointment of a new chief financial manager from private industry in January 2000. He has also hired a chief information officer, a senior acquisition executive, and created a transformation office. It is hoped that these officials will provide the capability for strategic planning and centralized coordination that NSA has been criticized for not maintaining. In July 2000 it was announced that William Black, Jr., a former NSA official who had retired and found employment in a high-tech consulting firm, Science Applications International Corporation, would be appointed deputy director. Black replaces Barbara McNamara who has been widely blamed in some media accounts[23] as part of an "old guard" that has delayed NSA's transition to post-Cold War challenges. McNamara has been assigned as head of NSA's liaison office in London.

In October 2000, further adjustments in NSA's management structure were announced. General Hayden will serve as Director and Chief Executive Officer and intends to focus on implementing the changes necessary to keep NSA relevant to the needs of the rest of the Government. Deputy Director Black will also serve as Chief Operating Officer and be responsible for day-to-day operations. A new Executive Leadership Team will be created to concentrate on overall strategic planning issues, composed of Hayden, Black, and the deputy directors for operations, information assurance, and technology.[24]

In June 2000 NSA announced that it intended to contract out "non-mission related" information technology (IT) support–information technology functions that are not part of its core cryptologic efforts.[25] A $4 billion IT contract, to be known as Project Groundbreaker, will be awarded for handling many of the Agency's extensive and varied requirements for information processing including desktop and workstation computers, email, network operations, software and telephone systems.[26] Hayden indicated that NSA divisions traditionally had undertaken much of their own IT work to support their ongoing operations, with inadequate concern for overall financial implications for the entire Agency. He was quoted in one account:

> I knew exactly how much activity X cost. I knew when we spent the money, I knew what it cost, I knew when it was appropriated. But we didn't really have the ability to aggregate all activity Xs and portray them to the agency as, "Hey, by the way, do you realize that is what activity X cost you around the world and do you really want to be spending [this] percentage of your budget on activity X as opposed to activity Y?" We couldn't do that. We couldn't pull the thread and

---

[23] Especially by Hersh, "The Intelligence Gap," p. 62.

[24] "NSA Chief Pushes Ahead with Overhaul," *Defense Information and Electronics Report*, October 20, 2000, pp. 1,4.

[25] For additional background on outsourcing issues, see Valerie Grasso, *Defense Outsourcing: the OMB Circular A-76 Policy*, CRS Report RL30392, April 12, 2000.

[26] Cahlink, "NSA May Outsource 5,000 High-Technology Jobs." The Request for Proposal for Groundbreaker is anticipated in January 2001 with the award of a contract in July 2001.

> aggregate what it was we were doing as an enterprise in order to make strategic decisions on direction.[27]

Hayden realizes that a more centralized system, with much work outsourced to a civilian contractor, may result in having to say "no to legitimate daily operational needs because the system can't handle it. That is the big change."[28]

Elements of Uncertainty

Few observers deny that significant structural changes in NSA's organization are warranted, but some caution that the changes thus far envisioned may not resolve the expected problems. Skeptics note, in particular, that outsourcing is no panacea, that it may mean the loss of experienced personnel with longstanding ties to NSA without necessarily reducing overall costs to the taxpayers. Further, they argue, the necessity of granting sensitive clearances to contractor personnel may increase risks of compromising classified information and processes. All agree that costs of background security investigations will increase.

Other objections may be raised concerning the consolidation of IT functions in a centralized office. The flexibility of individual components to design unique systems may be jeopardized, and the NSA Director has acknowledged that certain legitimate functions may have to be curtailed. Observers note that many of the technological advances in the past decade have been made by decentralized organizations that permit component divisions to establish their own operational practices and develop their own IT solutions without micro-management from a headquarters staff.

The External Team argued that "intelligence targets will continue to be increasingly transnational in nature, and . . . alignment to geographical locations and entities is obsolete." Although all observers would agree that NSA cannot maintain uniform depths of area expertise for all potential concerns, some suggest that there are areas that will be of intense concern to the U.S. Government for decades to come and dispersing area familiarities acquired over many years would be seriously mistaken.

Congressional observers strongly support the use of NSA's budget to establish priorities. They do not indicate that they believe NSA has mishandled funds; they do maintain that the Agency has not managed its budget to achieve managerial goals. In 1999 the House Intelligence Committee noted that "In the last two Congresses, the committee has been direct in its identification of process and management problems that required attention," but "NSA management has not yet stepped up to the line."

---

[27] Quoted in "NSA Overhauls Corporate Structure in Effort to Improve Operations," *Inside the Air Force*, June 23, 2000, p. 1.

[28] "NSA Overhauls corporate Structure to Improve Operations." Also, "NSA to Pursue Government-Industry Partnership for Information Technology Infrastructure Services," NSA Press Release, June 7, 2000.

The committee added that it "looks forward to the opportunities for change that present themselves with the introduction of a new Director of NSA."[29]

The Senate Intelligence Committee has urged that the NSA Director should have greater authority over the 70% of cryptologic resources that are currently managed by the military services. The military services operate collection sites, undertake initial analysis, and provide direct support to military commanders. NSA is responsible for tasking their efforts and for final analysis of the data they collect. Since service cryptologic elements support both NSA and military commanders there are inevitably differences over their disposition and responsibilities. Although the Senate Intelligence Committee advocates the NSA Director have "centralized direction across the SIGINT infrastructure as he implements his modernization strategy,"[30] some in DOD (and perhaps in Congress as well) would argue, however, that the need to configure sigint resources in direct support of operational commanders would argue against such augmented authorities for the leader of a Washington-area agency.

The House Committee, in reporting its version of the FY2001 Intelligence Authorization Act in May 2000 (H.R. 4392), accepted the need for managerial changes at NSA. Criticizing the traditional independence of NSA's divisions, the Committee argued that:

> Each type of communication–radio, satellite, microwave, cellular, cable–is becoming connected to all the others. Each new type of traffic shows up on every type of communication. Unfortunately, as the global network has become more integrated, NSA's culture has evolved so that is seemingly incapable of responding in an integrated fashion.

The House Committee argued that NSA must, as a result, "prepare itself for complex, prioritized, carefully timed and integrated systems acquisitions that, in aggregate, rival the complexity of programs commonly managed by the NRO, the Defense Department, and commercial industry."[31]

The House Intelligence Committee's recommendations for significant shifts in NSA's budget have not yet been accepted. DOD urged that the changes not be approved pending a review of the results of Hayden's initial reorganization efforts.[32] In particular, DOD, with support by the Senate Armed Services Committee, views with concern any efforts to give the DCI influence over NSA that would detract from that of the Secretary of Defense. These separate approaches may not easily be reconciled.

---

[29] H.Rept. 106-130, pp. 12-13.

[30] S.Rept. 106-279, p. 7.

[31] U.S. Congress, House of Representatives, 106th Congress, 2d session, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2001*, H.Rept. 106-620, p. 16.

[32] Letter from the Chairman of the Joint Chiefs of Staff and the Secretary of Defense to Chairman, Senate Armed Services Committee, reprinted in U.S. Congress, 106th Congress, 2d session, Senate, Committee on Armed Services, *Intelligence Authorization Act for FY 2001*, S. Rept. 106-325, pp. 8-9.

A major issue related to sigint in the post-Cold War environment is the erosion of distinctions between foreign and domestic threats. For example, an attack from outside the borders of the country through cyberspace could result in major damage to U.S. institutions, but responsibilities for monitoring potential threats are complex and in some ways ill-defined. Constitutional principles and statutes sharply distinguish between information gathering by foreign intelligence and domestic law enforcement agencies and efforts to involve NSA in surveillance of U.S. persons have been sharply restricted. Various administrative arrangements have been made to facilitate cooperation between NSA and the FBI and other law enforcement agencies in gathering information on threats with both foreign and domestic components, but many uncertainties remain. Many observers strongly oppose the use in court cases of information derived from sigint provided by NSA at the same time, sigint specialists are highly reluctant to see NSA diverted from its foreign intelligence missions to tasks that may risk involvement in domestic controversies. Congress, included in the FY20001 Intelligence Authorization bill (H.R. 4392, section 606) a requirement for a report from the Attorney General regarding actions taken in regard to the dissemination of intelligence information within the Justice Department. (This provision replaced an earlier version that would have required the establishment of procedures to accomplish this dissemination.)[33]

NSA and counterpart agencies in a number of other countries, especially Great Britain, have come under much criticism in the European Parliament for allegedly monitoring private communications of non-U.S. businessmen in a coordinated electronic surveillance effort known as Echelon in order to support domestic corporations. Some critics go further and charge that NSA's activities represent a constant threat to civil liberties of foreigners and U.S. persons as well. Though NSA has reassured congressional oversight committees that the Agency complies strictly with U.S. law, these controversies will undoubtedly continue.[34]

Conclusion

The National Security Act establishes sigint as a recognized function of the U.S. Government and requires that it is usually to be carried out by NSA. The U.S. Government thus has accepted responsibility for electronic surveillance activities that are condemned (but not necessarily eschewed) by some foreign countries. Although some specialists in international law argue that electronic surveillance is inherently illegal, U.S. officials contend, based on constitutional responsibilities, statutes, and long-established practice, that electronic surveillance related to national security and preventing terrorism and international narcotics smuggling is a legitimate function of the U.S. Government. Unlike some foreign countries, the U.S. has not asserted a right to conduct electronic surveillance to support its "economic well-being."

---

[33] See Richard A. Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS Report RL30252, July 2, 1999; also, J.M. McConnell, "The Future of SIGINT: Opportunities and Challenges in the Information Age," *Defense Intelligence Journal*, Summer 2000, especially pp. 46-47.

[34] For further information, see Appendix B.

Managing this effort in a changing geopolitical and technological environment, according to knowledgeable observers and congressional overseers, requires that NSA's organization and operations be substantially altered. This process is currently underway to strengthen the NSA Director's role in managing the Agency, but many uncertainties remain that will determine NSA's future. No national security official can confidently predict what collection priorities will exist in five years time, nor can the equipment acquisition priorities be firmly projected very far into the future. With congressional encouragement, the current leadership of NSA is drawing increasingly on talent available in the civilian community to offset the difficulties involved in retaining talented technological experts in a very tight sector of the labor market. This effort may not result in the stable, loyal workforce that, in the past, led to NSA's gradual successes against Cold War targets. Some observers also believe that NSA will ultimately require significant budgetary increases at a time when there is a determination to restrict overall government spending.

The future success of NSA is by no means guaranteed. The current NSA Director's managerial initiatives and the move to use outside contractors have widespread support, but these efforts may not achieve all their intended goals. NSA may not be adaptable to radically changing developments in international telecommunications and the bewildering emergence of terrorist groups previously unheard of. The wider public may come to view NSA's activities as inherent threats to privacy that outweigh the value of information acquired. Attention will be paid to the costs and benefits of allocating additional funds to NSA at a time when there are sure to be competing demands.

The current level of congressional concern with NSA is unlikely to diminish. Observers expect that, in the face of attacks on NSA by some in the media and by a number of European parliamentarians, members of Congress will be asked to defend or criticize not only NSA's operations, but also its statutory roles and missions. Funding for NSA's efforts to adapt to altered geopolitical and technological environments will have to be balanced against other competing needs. To a much greater extent than in the past, observers expect that Congress will continue to involve itself in internal changes in the Agency designed to acquire technological capabilities to acquire information at a time when the volume of communications is expanding exponentially, and access is greatly complicated by the spread of sophisticated encryption systems.

Appendix A. Congressional Oversight of NSA: A Brief Review

Codemaking and signals intelligence (sigint) have long been functions of governments and military organizations.[35] Although the United States gave less attention to codemaking and codebreaking than the major European powers, U.S. forces during World War I established a fairly extensive military sigint effort. In the 1920s and 1930s, the services maintained a small sigint effort and, for a time, the State Department collaborated with the Army in operating an American "Black Chamber" that attempted, with limited success, to intercept and decrypt foreign diplomatic communications. By the time the United States entered World War II, U.S. codebreakers were able to decrypt some codes of Japan, Germany, and other foreign countries. Success in breaking Japanese diplomatic codes, achieved through "the exercise of the greatest ingenuity and utmost resourcefulness" was acknowledged publicly after the end of the war in the congressional report regarding the attack on Pearl Harbor.[36]

During the course of World War II, sigint efforts proved to be exceptionally valuable especially in regard to acquiring military information. The crucial victory at Midway in June 1942 that halted Japan's advance in the Pacific was gained through sigint. The Allies' ability to keep supplies flowing across the North Atlantic depended on limiting U-boat attacks; this too was accomplished through good sigint. Some observers have concluded that sigint enabled the Allies to end the war at least a year earlier than would otherwise have been possible.

During World War II, cooperation with the British in sigint collection and analysis proved very fruitful. Although both countries were initially reluctant to share their codebreaking secrets, they gradually came to appreciate the advantages of sharing both collection and analysis. Anglo-American cooperation did not end with the conclusion of hostilities in 1945, but actually expanded with the beginning of the Cold War and the expansion of U.S. security interests throughout the world. The relationship with the British would eventually encompass the Canadians, Australians, and, to a lesser extent, the New Zealanders.

---

[35] For background, see David Kahn, *The Codebreakers: the Story of Secret Writing* (London: Weidenfeld and Nicolson, 1967). The first substantial description of NSA's activities was James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin, 1982). The creation of NSA is described in a 1952 document known as the Brownell Report that was later declassified and published as George A. Brownell, *The Origins and Development of the National Security Agency* (Laguna Hills, CA: Aegean Park Press, 1981).

[36] See U.S. Congress, 79th Congress, 2nd session Joint Committee on the Investigation of the Pearl Harbor Attack, *Investigation of the Pearl Harbor Attack*, Joint Committee Print, 1946, p. 179. Congressional pressure led the Truman Administration to authorize public release of information on the prewar sigint effort against Japan and the ensuing report included detailed discussion of sigint efforts prior to the Japanese attack since they were part of a major controversy surrounding the extent of preparedness at Pearl Harbor in 1941.

After the War, the Army and the Navy, and subsequently the newly independent Air Force all continued sigint collection. An effort was made to coordinate the services' sigint efforts in a single organization known as the Armed Forces Security Agency established by the Secretary of Defense in 1949. Coordination problems were not, however, resolved until October 1952 when President Truman established the National Security Agency in an effort to provide a more effective structure for coordinating signals intelligence activities. Truman had determined that the sigint function was "national," that it would serve civilian policymakers in the State Department and the White House as well as the military. This action was taken in a secret memorandum that was not made public at the time.

NSA became the U.S. focal point of a global sigint effort. Signals are collected at field stations throughout the world, most of which operated by the military services. Some initial processing and analysis may have be performed at the collection site, but in general the "take" is forwarded to NSA, which moved its headquarters from Arlington, Virginia to Fort Meade, Maryland in 1957. After decryption and analysis, the resultant data is provided to "all-source" intelligence agencies such as the CIA or the Defense Intelligence Agency (DIA). NSA has always been staffed by a combination of civil servants and active duty military personnel, but the Agency also provides operational guidance to sigint collection stations maintained by the cryptologic elements of the military services (collectively described as the Central Security Service (CSS)).

During the Cold War, NSA's operations, along with those of allied countries) were primarily directed at the Soviet Union, its Warsaw Pact allies, and Communist China. Massive efforts were made to collect sigint dealing with military threats to the U.S. and its allies. In addition to sigint provided to national-level decision makers, tactical sigint collection, analysis and reporting was incorporated in military operations, including those occurring in the Korean and Vietnam Wars.

For many years NSA's efforts did not receive much public scrutiny. Congressional oversight was conducted by small sub-committees of armed services and appropriations committees without public hearings. The first major legislation dealing directly with NSA was the National Security Agency Act of 1959 (P.L. 86-36). This Act did not describe the functions of NSA, but dealt with "housekeeping" matters such as pay and allowances, training, property acquisition, and leasing. It exempted NSA from the requirement to provide detailed information regarding organizational and functional matters to the Civil Service Commission (the predecessor of the Office of Personnel Management). These authorities are, in general, similar to those exercised by the Director of Central Intelligence (DCI) in regard to the CIA. The act has been amended from time to time and serves as the statutory basis for NSA's personnel policies that derive from its unique mission, including special pay and allowances for overseas travel, professional and foreign language training, and property leasing, and use of the NSA.

An exception to the practice of congressional reticence regarding NSA was a report on a widely publicized defection in 1960 of two NSA employees to the Soviet

Union.[37] The committee criticized personnel security procedures as shockingly lax and in part as a result of congressional criticism of the handling of the Mitchell/Martin case DOD tightened the security practices at NSA to ensure that background investigations were completed prior to granting access to cryptologic materials. In 1964 P.L. 88-290 (known as Title III of the Internal Security Act of 1950) was enacted to establish requirements for security investigations for persons working at NSA. Observers note that it was an early reflection of the importance of congressional oversight. It gave the NSA Director authority to terminate the employment of NSA personnel "whenever he considers that action to be in the best interest of the United States." Such actions can be taken notwithstanding usual civil service procedures for personnel actions. In 1996 these provisions were superseded by enactment of the FY1997 National Defense Authorization Act (P.L. 104-201, sections 1631-1635) which established intelligence personnel policies for the entire Defense Department, including authority to terminate employees "in the interests of the United States." Appeals of decisions to terminate can only be made to the Secretary of Defense.[38]

In the mid-1970s, public concerns that U.S. intelligence agencies were spying on domestic groups opposed to the Vietnam War led to hearings by select committees in both chambers.[39] Interest in NSA centered on "watch lists" that had been maintained to collect communications of U.S. citizens who were suspected of ties to hostile foreign countries and groups.[40] There was also interest in a project, known as Shamrock, by which copies of international telegrams were provided to NSA on a daily basis by three telegraph companies. These practices had been terminated by the early 1970's, but Members of Congress considered that the Agency should be held accountable for them.[41] (The desire to bring such practices under the constraints of statutory law contributed to passage of the Foreign Intelligence Surveillance Act of 1978.)

During the hearings conducted by the Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities (known as the Church Committee after its chairman, Senator Frank Church), for the first time a Director of NSA testified in open session to give a public overview of NSA's

---

[37] U.S. Congress, 87th Congress, 2d session, House of Representatives, Committee on Un-American Activities, *Security Practices in the National Security Agency (Defection of Bernon F. Mitchell and William H. Martin)*, Report [Committee Print], August 13, 1962.

[38] See General Accounting Office, *Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with those of Other Agencies*, GAO/NSIAD-96-6, March 1996.

[39] See Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence* (Chicago: Dorsey Press, 1988).

[40] See Morton H. Halperin *The Lawless State: the Crimes of the U.S. Intelligence Agencies* (New York: Penguin, 1976).

[41] See U.S. Congress, 94th Congress, 2d session, Senate, Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, Book III, 1976, pp. 765-776. The congressional investigation of Shamrock is described by a participant, L. Britt Snider, "Unlucky Shamrock: Recollections from the Church Committee's Investigation of NSA," *Studies in Intelligence*, Winter 1999-2000.

responsibilities. Lt. General Lew Allen, Jr., citing the statutory and other authorities under which NSA carried out its responsibilities, stated:

> This mission of NSA is directed to foreign intelligence, obtained from foreign electrical communications and also from other foreign signals such as radars. Signals are intercepted by many techniques and processed, sorted and analyzed by procedures which reject inappropriate or unnecessary signals. The foreign intelligence derived from these signals is then reported to various agencies of the government in response to their approved requirements for foreign intelligence.[42]

Allen also explained in some detail the practice of establishing "watch lists" by which "words, including individual names, subjects, locations, etc." could be identified within a stream of communications to separate useful information from the vast quantities of chatter. Particular attention was paid to retrieving information relating to terrorism, narcotics, and–a particular concern of the Johnson and Nixon Administrations–foreign influences on domestic groups suspected of fomenting civil disturbances in the U.S. in protest against the U.S. role in the Vietnam war.

Allen indicated that, pursuant to presidential direction, the Secretary of Defense had established NSA in accordance with his statutory authorities. He noted further that "for the past 22 years [i.e., since circa 1953], Congress has annually appropriated funds for the operation of the NSA, following hearings before the Armed Services and Appropriations Committees of both Houses of Congress in which extensive briefings of the NSA's signals intelligence mission have been conducted."[43]

The Church Committee concluded:

> The National Security Agency is one of the largest and most technically oriented components of the United States intelligence community. Its basic function is collecting and processing foreign communications and signals for intelligence purposes. NSA is also responsible for creating and supervising the cryptography of all United States Government agencies, and has a special responsibility for supervising the military services' cryptologic agencies. Another major responsibility is protecting the security of American communications.
>
> The Committee regards these functions as vital to American security. NSA's capability to perform these functions must be preserved. The Committee notes that despite the fact that NSA has been in existence for several decades, NSA still lacks a legislative charter. Moreover, in its extensive investigation, the Committee has identified intelligence community abuses in levying requirements on NSA and abuses by NSA itself in carrying out its functions. These abuses are detailed in the domestic portion of the Committee report. The Committee finds that there is a compelling need for an NSA charter to spell out limitations which will protect

---

[42] Testimony of Lt. Gen. Lew. Allen, Jr., Director, National Security Agency in U.S. Congress, 94th Congress, 1st session, Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Hearings, vol 5. *The National Security Agency and Fourth Amendment Rights*, 1976, p. 17.

[43] Ibid., p. 8.

individual constitutional rights without impairing NSA's necessary foreign intelligence mission.[44]

Thus, even a committee widely perceived as antagonistic to intelligence agencies concluded that NSA's sigint mission is "vital to American security." It urged, however, a better statutory framework for the Agency and an enhanced role for congressional oversight to ensure that NSA was not misused in ways that would undermine American liberties.

The complete final report of the House Select Committee on Intelligence (known as the Pike Committee) was never made public, but its published recommendations also included a proposal that the existence of NSA be recognized by specific legislation, that such legislation provide for civilian control of NSA, and that the role of NSA with reference to the monitoring of communications of Americans be defined.[45]

Many of the most important statutory provisions relating to NSA were enacted in the wake of these congressional investigations. Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) (50 USC 1801) which establishes procedures for electronic surveillance in the United States for foreign intelligence purposes.[46] It provides that the Attorney General may authorize surveillance in situations wherein the target is communications of foreign powers; in cases in which communications of U.S. persons might be acquired, then approval of a court, created pursuant to the FISA, would be required. Information acquired in accordance with FISA provisions is to be used for foreign intelligence purposes (even though in recent years Congress has expanded FISA to permit use of some types of information acquired under its provisions to be used for law enforcement purposes in certain circumstances). FISA, in essence, ensures that foreign intelligence electronic surveillance operations within the United States are conducted in accordance with statutory authorities and with supervision by the Justice Department (and with oversight by Congress)

Although in the Pearl Harbor investigations, the U.S. Government officially revealed its prewar sigint efforts, ongoing sigint activities had not been acknowledged. FISA provided authority in U.S. statutory law for electronic surveillance activities to be conducted for foreign intelligence (rather than law enforcement) purposes. In enacting the statute the United States Government accepted responsibility for NSA's activities no matter how they might be regarded in other countries. FISA does of course provide ample warning to foreign countries and foreign groups that the U.S. undertakes electronic surveillance when it perceives it necessary. While the argument

---

[44] U.S. Congress, 94th Congress, 2d session, Senate, Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Foreign and Military Intelligence, Book I*, Final Report, S.Rept. 94-755, April 26, 1976, p. 464.

[45] U.S. Congress, 94th Congress, 2d session, House of Representatives, Select Committee on Intelligence, *Recommendations of the Final Report of the House Select Committee on Intelligence*, H.Rept. 94-833, February 11, 1976, p. 3.

[46] See Elizabeth B. Bazan. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*, CRS Report RL30465, May 17, 2000.

was made that such activities are best undertaken without formal legal authorization and without the Government's accepting responsibility for them, Congress specifically rejected that argument in the belief that intelligence activities, including electronic surveillance, are necessary to protect the national security and that the U.S. Intelligence Community should be subject to law and to oversight by Congress.

In addition to FISA, there were also efforts to establish a "legislative charter" for the agencies of the Intelligence Community, including NSA. Testifying in February 1980, the then Director of NSA, Vice Admiral Bobby R. Inman, supported charter legislation, noting that "while the Agency has been provided with significant Congressional guidance and protection with respect to the information and products produced by the Agency, there was little Congressional guidance on the functions and responsibilities of the Agency and few Congressionally provided statutory tools to be used to perform those functions."[47] Charter legislation for the entire Intelligence Community became very complex and ultimately was a victim of partisan disputes in the late 1970s.[48] It was not until 1992 that the National Security Act was amended to provide a functional charter for NSA.[49] The Act now gives the Secretary of Defense the responsibility to ensure:

> through the National Security Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the conduct of signals intelligence activities and shall ensure that the product is disseminated in a timely manner to authorized recipients....

Guidance for NSA's activities has been further detailed in a series of executive orders.[50] E.O. 12333, signed by President Reagan on December 4, 1981 after extensive consultation with Congress, and still in effect, tasks the Secretary of Defense with responsibilities for NSA including:

> (1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense;
>
> (2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

---

[47] Testimony of B.R. Inman, Vice Admiral, U.S. Navy and Director of National Security Agency, U.S. Congress, 96th Congress, 2d session, Senate, Select Committee on Intelligence, *National Intelligence Act of 1980*, Hearings, 1980, p. 67.

[48] See John M. Oseth, *Regulating U.S. Intelligence Operations: A Study in Definition of the 0National Interest* (Lexington, KY: University Press of Kentucky, 1985).

[49] By the Intelligence Authorization Act for FY1993 (P.L. 102-496, section 705).

[50] The first, E.O. 11905, was issued by President Ford on February 18, 1976; the second, E.O. 12036, was issued by President Carter on January 24, 1978.

(3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;

(6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provisions of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence.

(8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;

(9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;

(10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;

(11) Prescribing, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;

(12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and

(13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement.

As noted above, in 1976 the Pike Committee urged civilian leadership for NSA. NSA has always been headed by military officers, but they have served under the direction of both the civilian Secretary of Defense and the (usually) civilian Director of Central Intelligence. In accordance with subsequent amendments to the National Security Act Directors of NSA are now appointed by the President upon the recommendation of the Secretary of Defense with the concurrence of the DCI (although a recommendation can be submitted without the DCI's concurrence if the

fact of non-concurrence is stated). In recent years, few observers express concerns about the NSA Director being a serving officer.

The amended National Security Act also provides that the DCI develops budgets for the annual National Foreign Intelligence Program which includes NSA. The DCI also establishes the requirements and priorities that govern the collection of national intelligence. These provisions provide authority for the DCI to oversee NSA's budget and operations. There are, however, multiple occasions for differences between the roles of the Secretary of Defense and the DCI. The Defense Secretary is inevitably more focused on aligning NSA closely with the operating forces of DOD and tends to emphasize collection of direct interest to military commanders. The DCI, for his part, tends to see NSA as one component of an interagency effort to gather intelligence for senior policymakers in Washington; he approves collection and analysis priorities that reflect their requirements. These respective responsibilities are well understood; defense and intelligence staffs attempt to make adjustments to accommodate differing requirements within budgetary constraints. Any major reorganization or redirection of efforts, however, that could affect NSA's ability to support either national policymakers or military commanders would be sure to generate criticism from one quarter or another.

The Pike and Church Committees also laid the groundwork for permanent intelligence committees. Subsequent to the establishment of the committees (the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence) in 1976-1977, Members and staff have regularly reviewed NSA programs and adjusted budgetary priorities with almost all hearings being conducted in closed sessions. NSA spending (along with the cryptologic activities of the services and other agencies) is authorized in annual intelligence authorization laws with funding levels indicated only in classified annexes. The two armed services committees also have oversight of most intelligence programs since they involved Defense Department assets.

Appendix B. Cooperation with Other Countries and the Echelon Controversy[51]

Although sigint collection and analysis are among the most sensitive activities undertaken by the U.S. Government, close cooperation in these efforts is maintained with several other countries–principally, but not limited to, the United Kingdom, Canada, Australia, and New Zealand. These relationships began during the Second World War when agreements to share signals intelligence were made between the military services of the United States and Great Britain, with separate arrangements made with other Commonwealth countries. This cooperation was widely considered by senior military leaders at the time, and by historians subsequently, with having significantly reduced the amount of time needed to defeat Nazi Germany and Japan as well as the number of Allied casualties. Although both the United States and Great Britain tackled various communications links of the Japanese and Germans (along with those of other countries), arrangements were worked out whereby the American effort was concentrated on the Japanese and the British on the Germans. The division of labor reflected resource limitations–especially among skilled cryptologists–and possession of geographical sites from which enemy transmissions could be intercepted.

With the end of hostilities in 1945, both British and American intelligence officials were reluctant to terminate a highly productive cooperative arrangement. There was continued military cooperation between the two countries in occupation duties in various areas and, when the Soviet Union began to be considered a threat to both countries, intelligence cooperation continued. Cooperation with Canada was considered essential in view of potential Soviet military activities originating in Arctic regions. Formal arrangements to cooperate in collecting and analyzing sigint were made by the two countries (and others) given shared geostrategic interests and limited resources that did not permit expansive unilateral efforts. These agreements were conducted in great secrecy at the time and remain largely classified a half-century later.[52]

The sigint relationship with the British and other Commonwealth countries has attracted criticism from a number of sources over the years.[53] To an extent a close intelligence relationships arguably predispose military and political leaders to

---

[51] See also Richard A. Best Jr., *Project Echelon: U.S. Electronic Surveillance Efforts*, CRS Report RS20444, Updated March 2, 2000.

[52] Post-World War II sigint cooperation with the British was authorized by President Truman as early as September 1945 in approving a recommendation by the Secretaries of State, War, and the Navy. See Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance," in Hayden B. Peake and Samuel Halpern, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (Washington: NIBC Press, 1994), pp. 104-105; also, Bradley F. Smith, *The Ultra-Magic Deals and the Most Secret Special Relationship* (Novato, CA: Presidio Press, 1993). Stephen Budiansky, "The Difficult Beginnings of US-British Codebreaking Cooperation," *Intelligence and National Security*, Summer 2000.

[53] See, for instance, Duncan Campbell, *The Unsinkable Aircraft Carrier: American Military Power in Britain* (London: Michael Joseph, 1984).

coordinated policies. Some observers object to international agreements made without the formal advice and consent of the U.S. Senate. The secret relationships have been criticized by observers in the U.S., Britain, Australia and elsewhere who oppose international entanglements. Some observers from European Union countries express concern that sigint cooperation among the "Anglo-Saxons" might work against their own economic interests.

Supporters of the such relationships with other countries point to the advantages in shared efforts that conserve intelligence resources. The United States, Britain, Canada, Australia, and New Zealand often have common policies on important international issues, but the existence of close intelligence ties has not precluded different policies (or even, as at Suez in 1956, opposing policies) when national leaders felt them necessary. In the post-Cold War environment, observers believe that sigint cooperation with a number of friendly countries maximizes opportunities to obtain information regarding disparate regional threats from terrorist groups, narcotics traffickers, and dealers in nuclear and other substances used in making weapons of mass destruction.

NSA has long been the target of criticism from those who view intelligence agencies as inevitable threats to civil liberties. In general, however, the Agency's low public profile and the esoteric nature of its work attracted less attention than the more dramatic covert actions undertaken by the CIA. In the past few years, however, reports prepared under the auspices of the Directorate-General for Research of the European Parliament have described U.S. electronic surveillance efforts. The studies, known as Scientific and Technological Options Assessments (STOA), are prepared by contractors and not by European Parliament's official staff. A series of these reports have severely criticized NSA, charging it with working together with sigint organizations of the United Kingdom, Canada, Australia, and New Zealand to gather commercial communications and providing the intercepts to U.S. business interests to give them advantages over foreign firms.[54]

The criticisms of NSA by these reports have been echoed by media commentary. One account claims that

> It is the new Cold War. The United States intelligence agencies, facing downsizing after the fall of the Berlin wall, have found themselves a new role spying on foreign firms to help American business in global markets.
>
> Echelon is part of a British and American-run world-wide spy system that can "suck up" phone calls, faxes and e-mails sent by satellite. America's intelligence agencies have been able to intercept these vital private communications, often between foreign governments and European businesses, to help the US win major contracts.[55]

---

[54] See especially *Interception Capabilities: Report to the Director General for Research of the European Parliament*, Scientific and Technical Options Assessment Programme Office, European Parliament, April 1999.

[55] Duncan Campbell and Paul Lashmar, "The New Cold War: How America Spies on Us for

(continued...)

Some media accounts state that this entire cooperative endeavor has the codename Project Echelon; others believe that Echelon refers only to the process by which computers operated by cooperating sigint agencies sift through many thousands of intercepts for ones containing pre-programmed key words.[56]

U.S. intelligence officials have responded to these charges by describing the statutory framework under which NSA operates and the oversight mechanisms in place in both the Executive and Legislative Branches. There have been categorical denials that intelligence is passed to U.S. companies to provide them commercial advantages although it is freely acknowledged that sigint is used to provide the U.S. Government with information about bribery and other illegal practices of foreign firms and that this information has been used as the basis for diplomatic complaints.[57]

NSA has successfully persuaded the congressional leadership that it faithfully and responsibly conducts its electronic surveillance activities in accordance with law and relevant executive orders. Section 309 of the Intelligence Authorization Act for FY2000 (P.L. 106-120) required that the Director of NSA submit a report (to be prepared jointly by the Director of NSA, the DCI, and the Attorney General) providing a detailed analysis of the legal standards used in conducting signals intelligence activities, including electronic surveillance. The report was submitted in February 2000 and set forth the legal bases for NSA's activities, emphasizing its commitment to respect the privacy rights of U.S. persons. In a public hearing to discuss the report, Representative Goss, Chairman of the House Intelligence Committee, concluded that "our safeguards are in place and are working."[58]

Most U.S. observers give credence to the official U.S. position, especially given the absence of evidence that U.S. companies are pressuring the Government for help in learning about foreign technologies. Observers suggest, in addition, that any U.S. intelligence assistance to a U.S. firm in winning a foreign contract would provoke strong criticism by a disadvantaged U.S. competitor.[59] Former DCI R. James

---

[55] (...continued)
its Oldest Friend–the Dollar," *Independent* (London), July 2, 2000. Campbell and Lashmar detail instances in which the U.S. Government complained to foreign countries that European firms were attempting to bribe their officials and, as a result, the contracts ultimately went to U.S. firms. They quote others as maintaining that U.S. officials pass intelligence information directly to U.S. corporations.

[56] See Jeffrey Richelson, "Desperately Seeking Signals,"*Bulletin of Atomic Scientists*, March/April 2000.

[57] "With respect to allegations of industrial espionage, the notion that we collect intelligence to promote American business interests is simply wrong. We do not to [*sic*] target foreign companies to support American business interests." Federal News Service, Prepared Testimony of George J. Tenet, Director of Central Intelligence Before the House Committee on Intelligence, April 12, 2000, p. 4.

[58] Federal News Service, Hearing of the House Permanent Select Committee on Intelligence, April 12, 2000, p. 33.

[59] There is no provision in U.S. law for foreign intelligence agencies to assist U.S. firms and
(continued...)

Woolsey has maintained that U.S. intelligence agencies do not collect information about foreign technology because American technology is, in general, far superior. There is, however, he argues, a real need to seek information about corrupt practices by foreign competitors and activities such as transfers of dual-use technologies for use in production of weapons of mass destruction as well as activities in countries subject to U.N. sanctions.[60]

Some foreign observers continue to dispute U.S. claims and they will not easily be persuaded that their concerns are ill-founded. Suggestions of NSA electronic eavesdropping have clearly had resonance among members of the European Parliament which voted on July 5, 2000 to undertake a lengthy investigation of Echelon. The investigation will not include the calling of witnesses and, interestingly, an amendment calling for an investigation of eavesdropping by all EU governments was not adopted.[61] In part, foreign objections stem from concern about the capabilities of NSA to monitor their communications and those of European companies. There is also, especially among some, irritation that the United States has a closer sigint relationship with some of its allies than with others. In part, however, observers perceive attacks on NSA's activities as instinctive hostility among political elements long skeptical of close U.S.-European relations and determined to forge a more independent European identity. Some objections also undoubtedly arise from deep-seated opposition to the work of all intelligence agencies.

There is no question that the worldwide capabilities of NSA cause suspicion and resentment among some foreign elements. U.S. officials justify NSA's activities on international law, the necessity to acquire information about threats to national security, international terrorism, and the narcotics trade. While the potential for abuse is acknowledged, the United States has a legal structure that regulates electronic surveillance. In addition, intelligence derived from sigint supports many collective military and diplomatic efforts with European and other allies.

---

[59] (...continued)
there are important privacy protections mandated by FISA. On the other hand, Article 8 of the European Convention on Human Rights recognizes a right of privacy that is not to be interfered with except as is necessary in "the interests of national security, public safety or the *economic well-being* of the country." (Emphasis added.) The full implications of this provision are uncertain, but it would not necessarily preclude the interception of communications by intelligence agencies to obtain commercial advantages for their country's businesses.

[60] R. James Woolsey, "Why We Spy on Our Allies," *Wall Street Journal*, March 17, 2000.

[61] Ambrose Evans-Pritchard, "GCHQ Faces Inquiry over US 'Spying' on Europe," *Electronic Telegraph*, July 6, 2000.