Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)
Chief Information Officer

TRANSITION BOOK

Prepared: December 22, 2000

Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)
Chief Information Officer (ASD(C3I)/CIO)

I. ORGANIZATION AND MANAGEMENT

A. Organization

1. Mission Statement
2. Organization Structure
3. Goals
4. Functions

B. Management

1. Chain of Command
2. Regulatory Authority
3. Management Studies and Issues (studies that focus on organizational structure or operation)

C. External Process

1. Executive – Key Interagency Relationships
2. Congressional

a. Key Committees
b. Critical Reports to Congress
c. Pending Legislative Issues

II. BUDGET

A. Budget Overview
B. Budget Details
C. Budget Trends
D. Budget Issues

III. PERSONNEL

A. Summary of Statistics
B. Personnel Management Issues

IV. POLICY/ISSUES

A. Overview of the Policy Development Process
B. Major Policy Issues requiring attention in the next few months

I. Organization & management

A. Organization

Mission Statement

ASD(C3I)/CIO
Vision and Mission

VISION: Make Information Superiority Happen

MISSION: Establish policy provide guidance and oversight, and leverage technology to achieve Information Superiority for the warfighter and the Department's business processes and to maintain and strengthen national security.

The ASD(C3I)/CIO is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for a wide range of areas, including:

- command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR);
- space and space-related activities;
- airspace matters and military air-traffic control policy;
- counterintelligence;
- Information Management and Information Technology;
- information operations, assurance, and superiority;
- electronic business and commerce;
- personnel, industrial, physical, and classification security matters;
- imagery, imagery intelligence, mapping, charting, and geospatial matters;
- frequency spectrum management;
- critical infrastructure protection; and
- information interoperability.

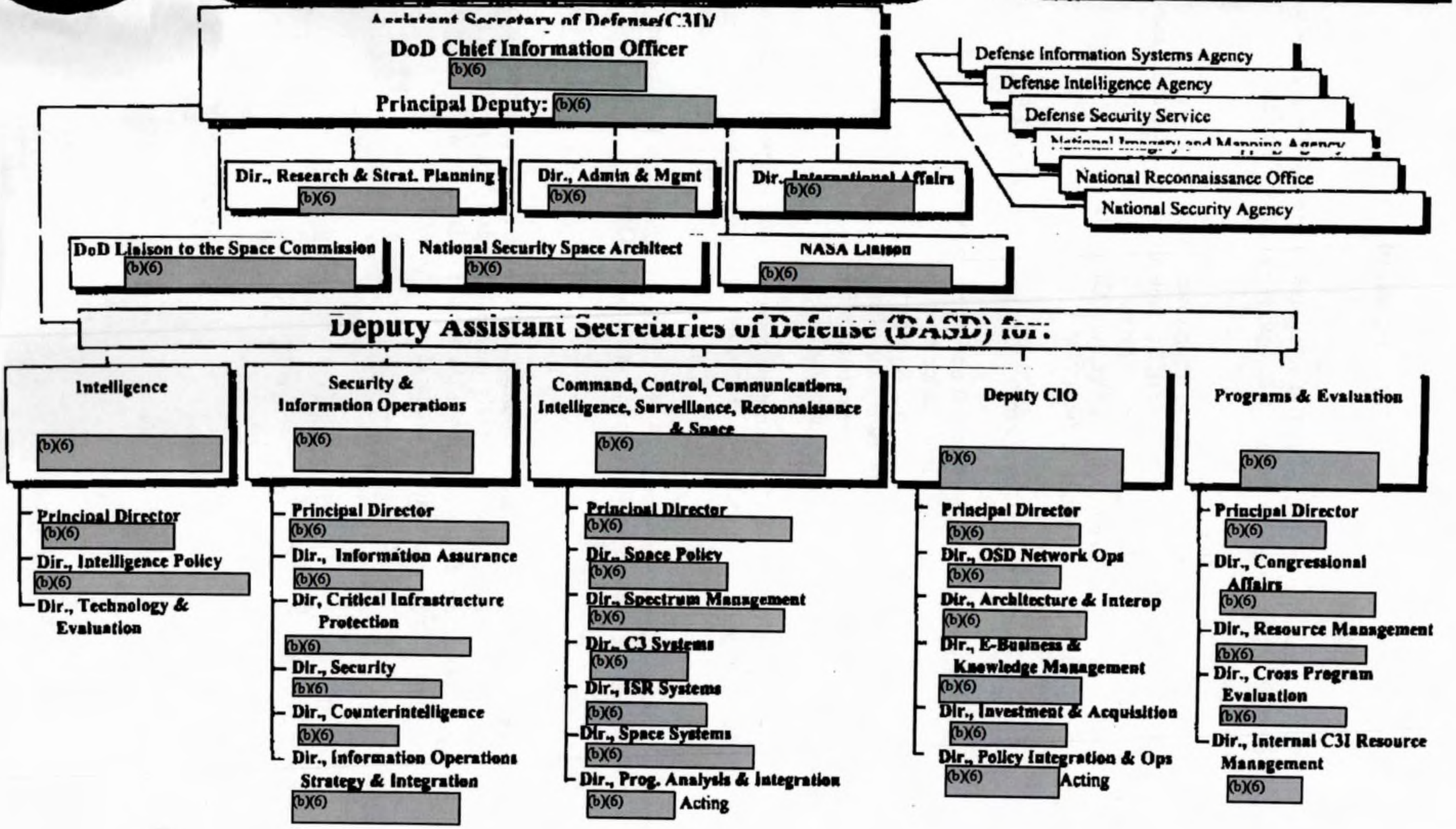
As the CIO, the ASD(C3I) is the Department's chief information resources official and is charged with managing Information Management (IM) and Information Technology (IT) responsibilities and functions pursuant to the Clinger-Cohen Act of 1996.

Organization Structure

Goals

OASD C3I

OASD(C3I) Organization



Assistant Secretary of Defense(C3I)/
DoD Chief Information Officer
(b)(6)
Principal Deputy: (b)(6)

Defense Information Systems Agency
Defense Intelligence Agency
Defense Security Service
National Imagery and Mapping Agency
National Reconnaissance Office
National Security Agency

Dir., Research & Strat. Planning
(b)(6)

Dir., Admin & Mgmt
(b)(6)

Dir., International Affairs
(b)(6)

DoD Liaison to the Space Commission
(b)(6)

National Security Space Architect
(b)(6)

NASA Liaison
(b)(6)

Deputy Assistant Secretaries of Defense (DASD) for:

Intelligence
(b)(6)
- Princioal Director
(b)(6)
- Dir., Intelligence Policy
(b)(6)
- Dir., Technology & Evaluation

Security & Information Operations
(b)(6)
- Principal Director
(b)(6)
- Dir., Information Assurance
(b)(6)
- Dir, Critical Infrastructure Protection
(b)(6)
- Dir., Security
(b)(6)
- Dir., Counterintelligence
(b)(6)
- Dir., Information Operations Strategy & Integration
(b)(6)

Command, Control, Communications, Intelligence, Surveillance, Reconnaissance & Space
(b)(6)
- Princioal Director
(b)(6)
- Dir., Space Policy
(b)(6)
- Dir., Spectrum Management
(b)(6)
- Dir., C3 Systems
(b)(6)
- Dir., ISR Systems
(b)(6)
- Dir., Space Systems
(b)(6)
- Dir., Prog. Analysis & Integration
(b)(6) Acting

Deputy CIO
(b)(6)
- Principal Director
(b)(6)
- Dir., OSD Network Ops
(b)(6)
- Dir., Architecture & Interop
(b)(6)
- Dir., E-Business & Knowledge Management
(b)(6)
- Dir., Investment & Acquisition
(b)(6)
- Dir., Policy Integration & Ops
(b)(6) Acting

Programs & Evaluation
(b)(6)
- Principal Director
(b)(6)
- Dir., Congressional Affairs
(b)(6)
- Dir., Resource Management
(b)(6)
- Dir., Cross Program Evaluation
(b)(6)
- Dir., Internal C3I Resource Management
(b)(6)

ASD(C3I)/CIO Organizational Structure

The Office of the ASD(C3I)/CIO is divided into five Deputy Assistant Secretariats, as shown on the attached organization chart. They are:

- Intelligence
- Security & Information Operations
- Command, Control, Communications, Intelligence, Surveillance, Reconnaissance & Space
- Deputy Chief Information Officer
- Programs & Evaluation

In addition, six agencies report through the ASD(C3I)/CIO:

- Defense Information Systems Agency
- Defense Intelligence Agency
- Defense Security Agency
- National Imagery and Mapping Agency
- National Reconnaissance Office
- National Security Agency

Also reporting to the ASD(C3I) are the National Security Space Architect, the National Aeronautics Space Association Liaison, and the DoD Liaison to the Space Commission.

More detail is available on the A-Net (http://anet.c3i.osd.mil/). Passwords for access to this network have been provided to the Transition Office.

The current organizational structure of ASD(C3I)/CIO was implemented in January 1999. However, the essence of this principal staff assistant has existed in various titles and organizational structures in the Department of Defense since 1970. A detailed history of this organization is available on our web site.

ASD(C3I)/CIO Goals

Information Superiority is the most important contribution that the ASD(C3I)/CIO community makes to the realization of Joint Vision (JV) 2010 and 2020. There are several definitions of Information Superiority but, in essence, Information Superiority is getting the right information, to the right person, at the right time, in the right format while denying your opponent the same advantages. Information Superiority is a key enabler of the operational concepts of Precision Engagement, Dominant Maneuver, Focused Logistics, and Full Dimensional Protection. To promote IS the Office of the ASD(C3I)/CIO has laid out a series of goals for the organization, which are reviewed closely by senior management.

ASD (C3I) Goals Toward Achieving Information Superiority

Implement effective programs for establishing Information Assurance (IA) and Critical Infrastructure Protection (CIP).

Goal definition: This goal is specifically aimed at protecting DoD's information assets and the information processes necessary for mission accomplishment. Information Assurance requires that key data bases maintain their integrity, information is available when needed, confidentiality can be maintained, we can identify and authenticate those on the networks and electronically signed contracts can be made binding (non-repudiation). To meet this goal we must continuously identify and analyze the interdependency of our assets; train and certify personnel; improve operations to ensure a secure operating environment; and leveraging technology.

Build a coherent, secure, integrated global network.

Goal definition: The coherent global network, referred to as the Global Information Grid (GIG), is aimed at ensuring the delivery of secure, assured, effective, and interoperable information to the warfighter and the various agencies that provide national security.

Plan and implement joint and combined end-to-end C3ISR and space integration.

Goal definition: This goal is centered on guiding the development and integration of advanced capabilities for C3ISR; space control; space support; weather; tracking and navigation. As with the previous goal, the main focus is to promote interoperability. Meeting this goal includes developing processes, which achieve cross-program integration and improve joint and combined interoperability. Through these efforts we also are better able to defend those parts of the radio frequency spectrum of importance to DoD, as well as to update and expand DoD policy to meet the growing importance of space to the warfighter.

Promote the development of knowledge management and a skill-based workforce throughout DoD

> **Goal definition:** Information Superiority is about much more than systems and technology, it is also about people and their thought processes. Implicit in the phrase "the right information in the right forms" is the need to turn information into awareness, knowledge and understanding. This goal is aimed at applying modern methodologies to transform data into just-in-time, reusable knowledge-bases, and developing a skill-based workforce capable of building, securing, maintaining, and applying information technology to achieve process change and information superiority.

Ensure the defense intelligence capabilities necessary for information superiority.

> **Goal definition:** The Intelligence Community has much to offer DoD and we have significantly improved our ability to make all information products available to warfighters in a timely manner, but much more needs to be done. This goal seeks to reinvent intelligence for the 21st Century, guiding the development and implementation of a ready and responsive intelligence force which is able to collect, analyze and exploit information efficiently and effectively at all levels of sensitivity and provide it to all consumers, according to their needs.

Strengthen the Information Operations (IO), Security, and Counterintelligence (CI) posture of the DoD.

> **Goal definition:** The Information Age doubtless will bring new forms of warfare. It is clear that we do not yet fully appreciate the potential and nature of Information Operations, the emerging threats to security, and the measures we need to take to counter these threats. This goal addresses those policies, program implementations, and resource allocations which enable the protection of critical DoD assets, anticipation and detection of threats and attacks upon those assets, application of appropriate responses, integration of IO into DoD planning and operations, and the maintenance and promotion of information superiority.

Promote electronic business/electronic commerce (EB/EC) and business process change throughout DoD.

> **Goal definition:** We are all aware of the changes that are taking place in the business world -- how we communicate, bank, shop, conduct business-to-business transactions and entertain ourselves. DoD needs to keep abreast of such new ways of doing the business and modify the Department's procurement, financial, logistics, and other practices accordingly. This goal seeks to promote electronic business/electronic commerce and business process change.

Foster development of an advanced technology plan for information superiority

> **Goal definition:** For many years DoD was the leader in most areas of technology. Today, particularly in information- related technologies, this is not the case. The commercial sector is setting the pace in both technology and its application. However, all of our needs will not be met simply by buying commercial-off-the shelf (COTS) products and services. To make sure DoD has taken the prudent steps to ensure we will have the technology we will need to support JV 2020, we are developing an advanced technology plan for Information Superiority in conjunction with USD(AT&L), DARPA and others. This plan provides guidance and focus to current and emerging DoD and commercial research and development and defines the needed capabilities and associated technology leading to the achievement of information superiority.

Underpinning all of these goals is the Foundation Goal which focuses on our people. By taking care of our people, we inspire, and sustain a highly motivated team that is committed to achieving information superiority.

> **Goal definition:** ASD(C3I)/CIO management efforts are focused on developing and maintaining a qualified motivated and diverse workforce especially within OSD. This includes continuously assessing and enhancing employee skills, as well as promoting career development. Internal administrative processes have been reviewed and updated to reflect clear and practical operating procedures.

Functions

OASD(C3I)/CIO Functions

DASD/Command, Control, Communications, Intelligence Surveillance Reconnaissance & Space

The DASD for Command, Control, Communications, Intelligence Surveillance Reconnaissance & Space (C3ISR&S) serves as the principal advisor to the ASD (C3I) for strategic, tactical, and defense-wide C3 activities and systems.

- Guides the development and integration of defense capabilities for communications, command and control, intelligence, surveillance, reconnaissance, space control, and space support
- Responsible for space policy and spectrum management
- Reviews all proposed C3ISR and space systems programs in terms of total DoD requirements, technology, and availability of resources
- Makes recommendations on program trade-offs, systems integration, and consolidation

DASD/Intelligence

The DASD for Intelligence (I) provides the primary staff policy oversight function of DoD intelligence activities.

- Supervises the development of Defense intelligence policy and planning guidance;
- Monitors the DoD intelligence requirements process
- Governs the programming and budgeting functions relative to DoD interests in the National Foreign Intelligence Program (NFIP) and the reconciliation of those interests with Tactical Intelligence and Related Activities (TIARA) and the Joint Military Intelligence Program (JMIP) of the Department
- Assesses customer satisfaction and oversees the performance of the various elements of defense intelligence
- Provides programmatic, technical, and policy advice and assistance to the ASD (C3I) on current and future issues pertaining to intelligence and intelligence-related activities, with concentration on issues related to modernization planning, research and development efforts, acquisition matters, command support, and personnel policy
- Responsible for development of the intelligence portion of the Secretary of Defense's guidance
- Conducts technical reviews of intelligence and intelligence-related systems and programs during development and acquisition
- Leads system performance evaluations and preparation of annual budget requests to Congress

OASD(C3I)/CIO Functions (continued)

DASD/Security and Information Operations

The DASD for Security and Information Operations (S&IO) is responsible for creating, maintaining, and overseeing the execution of Defense-wide policy and programs aimed at assuring the security, reliability, and protection of DoD's mission essential personnel, information, networks, facilities, and supporting infrastructures. Specific functional areas include:

- Physical, personnel, information, operational, and technical security
- Information Assurance
- Critical Infrastructure Protection (both physical and cyber)
- Information Operations
- Counterintelligence

DASD/Deputy Chief Information Officer

The Deputy Chief Information Officer (DCIO) is responsible for ensuring that the Department's management and acquisition of information technology (IT) is in compliance with the Clinger-Cohen Act.

- Provides overall direction and guidance for managing information resources
- Promotes the effective and efficient design and operation of all major information management processes, including work process improvements
- Develops, maintains and facilitates the implementation of an integrated information technology architecture for the department
- Designs and implements a process for maximizing the value and assessing and managing the risks of information technology acquisitions
- Monitors and evaluates the performance of IT programs
- Advises the Secretary of Defense regarding whether to continue, modify, or terminate a program or project; and providing recommendations to the Secretary on budget requests for IT, including national security systems

DASD/Programs and Evaluation

The DASD for Programs and Evaluation (P&E) serves as the principal advisor to the ASD (C3I) and lead office developing integrated Departmental and legislative Information Superiority strategies through comprehensive resource and programmatic evaluations, assessments and prioritized recommendations.

- Advises the ASD (C3I) on Information Superiority resource, legislative and congressional issues
- Assesses the Military Service and Defense Agency proposed programmatic solutions against validated and prioritized requirements
- Fosters the establishment of program and budget priorities of the Military Services and Defense Agencies to build Information Superiority through the resource processes
- Champions ASD (C3I) participation in program and budget reviews with key DoD leaders
- Generates legislative strategies to achieve Information Superiority
- Manages and oversees all internal C3I resources

B. Management

Chain of Command

ASD(C3I)/CIO Chain of Command

The ASD(C3I)/CIO reports directly to the Secretary of Defense. For matters related to acquisition of major systems, ASD(C3I) CIO reports through the USD (Acquisition, Technology & Logistics) to the Secretary of Defense

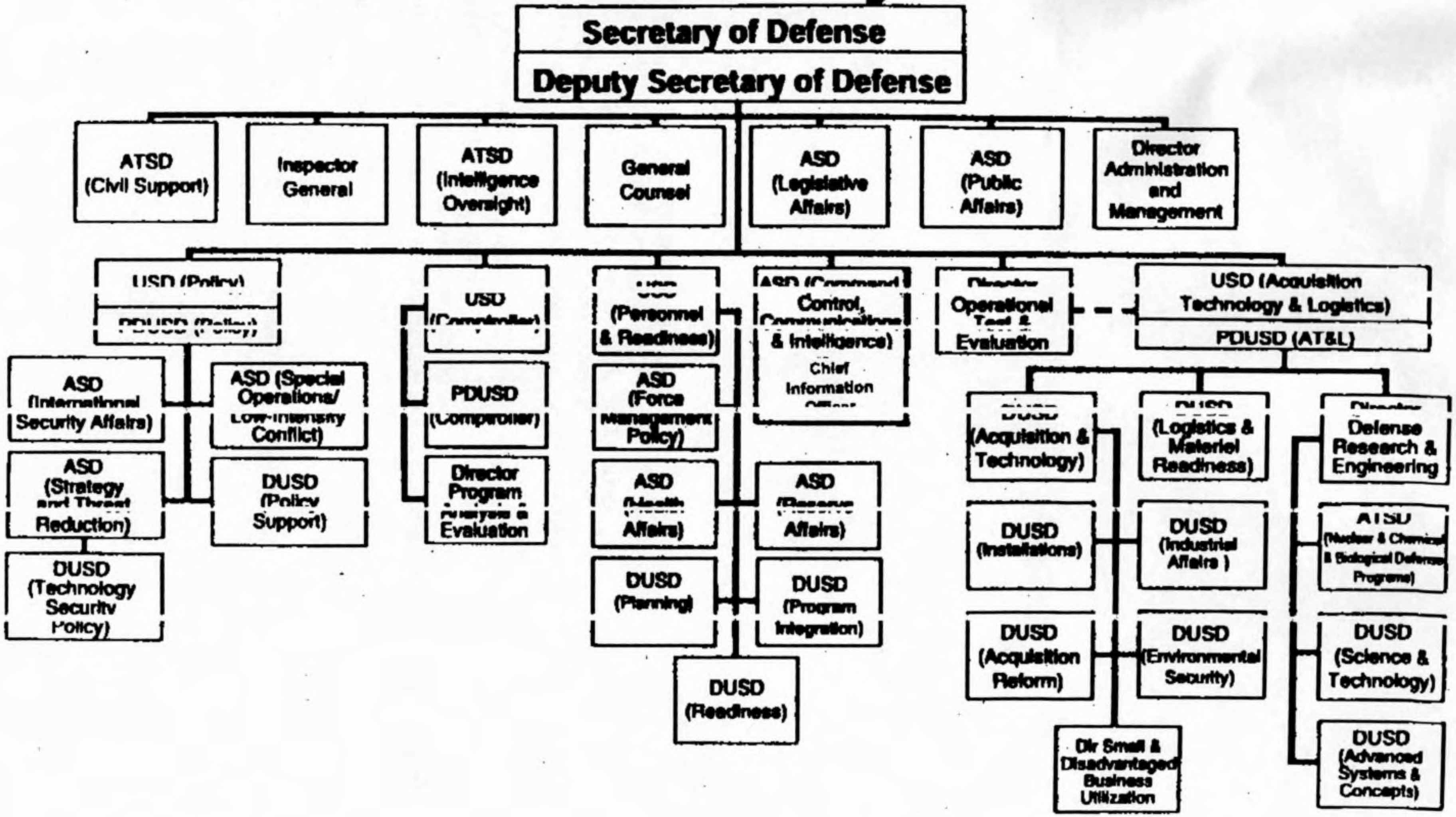
In addition, the ASD(C3I)/CIO:

Exercises authority, direction and control over three Defense Combat Support Agencies:
Defense Information Systems Agency
Defense Intelligence Agency
Defense Security Service

Exercises overall staff supervision four other Defense Components:
National Imagery and Mapping Agency
National Security Agency/Central Security Service
National Reconnaissance Office
The National Security Space Architect

CHAIN OF COMMAND

Office of the Secretary of Defense



Secretary of Defense
Deputy Secretary of Defense
ATSD (Civil Support)
Inspector General
ATSD (Intelligence Oversight)
General Counsel
ASD (Legislative Affairs)
ASD (Public Affairs)
Director Administration and Management
USD (Policy)
PDUSD (Policy)
ASD (International Security Affairs)
ASD (Special Operations/ Low-Intensity Conflict)
ASD (Strategy and Threat Reduction)
DUSD (Policy Support)
DUSD (Technology Security Policy)
USD (Comptroller)
PDUSD (Comptroller)
Director Program Analysis & Evaluation
USD (Personnel & Readiness)
ASD (Force Management Policy)
ASD (Health Affairs)
ASD (Reserve Affairs)
DUSD (Planning)
DUSD (Program Integration)
DUSD (Readiness)
ASD (Command Control, Communications & Intelligence)
Chief Information Officer
Director Operational Test & Evaluation
USD (Acquisition Technology & Logistics)
PDUSD (AT&L)
DUSD (Acquisition & Technology)
DUSD (Logistics & Materiel Readiness)
Director Defense Research & Engineering
DUSD (Installations)
DUSD (Industrial Affairs)
ATSD (Nuclear & Chemical & Biological Defense Programs)
DUSD (Acquisition Reform)
DUSD (Environmental Security)
DUSD (Science & Technology)
Dir Small & Disadvantaged Business Utilization
DUSD (Advanced Systems & Concepts)

Date: February 2000

Regulatory Authority

Regulatory Authority of the ASD(C3I) CIO

Under the authority, direction and control of the Secretary of Defense, the ASD(C3I)/CIO really operates under two distinct sets of authorities. The first relates to the role as the ASD(C3I), the second to the CIO duties. There is considerable synergy between the two but the statutory basis is different.

ASD(C3I)

The ASD serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary for achieving and maintaining Information Superiority. The basis for Information Superiority is the collection, processing and dissemination of an uninterrupted flow of information in support of DoD missions, while exploiting or denying an adversary's ability to do the same. This entails a wide range of responsibilities from security and critical infrastructure protection to command, control and communication, space activities, intelligence and electronic commerce.

- The ASD(C3I)'s duties are described in DoD Directive 5137.1, of February 1992. However, this does not mention many functions that have been added in recent years, including those of the CIO. An updated version of the directive has been coordinated throughout the Department, but the DCI has challenged the Secretary's delegation to the ASD of certain oversight functions related to various intelligence agencies (NSA, NRO and NIMA). Accordingly, the revised directive has not been signed.

- In addition to duties assigned by the Department the ASD has several tasks that stem from Executive Orders (E.O.) and Presidential Decision Directives (PDD). These include:
  - DoD Executive Agent for the National Communications System (E.O. 12472).
  - DoD Chief Infrastructure Assurance Officer (CIAO), and SecDef's representative as the Functional Coordinator for National Defense infrastructures (PDD 63).
  - Executive Agent for the National Industrial Security Program (E.O. 12829).
  - Senior official to develop and oversee DoD policies regarding the classification and safeguarding of national security information -- including special access programs and security education and awareness, (E.O. 12958 & 12958).
  - Oversight of DoD responsibilities concerning counterintelligence and national intelligence activities, (E.O. 12333) including the Foreign Counterintelligence Program and the Security and Investigative Activities Program.
  - DoD focal point for the Federal Aviation Administration (FAA) and its transfer to the DoD under certain national security emergencies (E.O. 11161).
  - Other responsibilities as defined in PDDs with classified titles.

Besides the Executive Branch authorities mentioned above, the statutory authorities stem from Title 10 for DoD activities and Title 50 for intelligence missions.

CIO

In 1996, the Deputy Secretary designated the ASD(C3I) as the DoD CIO. Subsequently, the Secretary designated the DoD CIO as the PSA for DoD information management, information resources management, and information technology (IM/IRM/IT) matters (reference (e)), and delegated to the DoD CIO all of the duties and authorities given to the Agency Head in the Clinger-Cohen Act of 1996 (CCA). The DoD Appropriations Act of 1999 enhanced the CIO's Title 10 budgetary authority. By law, the CIO reports directly to the Secretary and Deputy Secretary.

Overall, the DoD CIO is responsible for providing advice and other assistance to the Secretary and other DoD senior management personnel to ensure that information technology is acquired and information resources are managed in a manner that implements the policies and procedures of references (a) through (d), and the priorities established by the Secretary.

The DoD CIO has four key responsibilities within his assigned functional area (i.e., IM/IRM/IT). These are: (1) policy development, (2) planning, (3) resource management, and (4) fiscal and program evaluation and oversight to assure the effective allocation and efficient management of resources consistent with approved policies, plans, and programs. Specifically:

- Policy - Develop DoD IM/IRM/IT policies and procedures including, but not limited to, those addressing process change, IT architectures, interoperability of IT (including National Security Systems (NSS)), and IT and NSS standards (CCA, Title 10, and SecDef Memo).

- Planning - Develop a DoD strategic plan that addresses the management and use of IT capabilities and proves overall direction and guidance for managing DoD's information resources (CCA and Paperwork Reduction Act).

- Resources Management
  - Review and provide recommendations to the Secretary on budget requests for IT and NSS investments (CCA, Title 10, and SecDef Memo);
  - Provide for the elimination of duplicate IT and NSS within and between the Military Departments and Defense Agencies (CCA, Title 10, and SecDef Memo);
  - Design and implement DoD process for maximizing the value and assessing and managing the risks of IT acquisitions (CCA and SecDef Memo);
  - Institutionalize performance-based and results-based management for IT (CCA and SecDef Memo); and
  - Develop strategies and plans for educating, training, and maintaining an adequate IRM workforce (CCA, Paperwork Reduction Act and SecDef Memo).

- Oversight
  - Provide management and oversight of all DoD IT, including NSS (CCA, SecDef Memo);
  - Monitor the performance of IT programs, evaluate the performance of those programs on the basis of applicable performance measurements, and advise the Secretary regarding whether to continue, modify, or terminate a program or project (CCA, Title 10, and SecDef Memo); and
  - Identify any major IT acquisition program that has significantly deviated from the cost, performance, or schedule goals (CCA, SecDef Memo).

References:

ASD(C3I)

Titles 10 and 50 United States Code
National Security Act of 1947
PDD/NSC 63, "Critical Infrastructure Protection," May 22, 1998
E.O. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984
E.O. 12958, "Classified National Security Information," April 17, 1995
E.O. 12829, "National Industrial Security Program," January 6, 1993
E.O. 12968, "Access to Classified Information," August 7, 1995
E.O. 12333, "United States Intelligence Activities," December 4, 1981
E.O. 11161, "Relating to Certain Relationships Between the Department of Defense and the Federal Aviation Administration," July 7, 1964, as amended by Executive Order 11382
Other PDDs with classified titles

CIO:

(a) Clinger-Cohen Act of 1996
(b) Chapter 131 of Title 10, Section 2223, "Additional Information Technology Responsibilities of Chief Information Officers"
(c) Paperwork Reduction Act
(d) Executive order 13011, "Federal Information Technology," dated July 16, 1996
(e) SecDef memo, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," dated June 2, 1996

Management Studies And Issues

ASD(C3I)/CIO Management Issues
Defense Reform Initiatives (DRIs) 1997/1998

The functions and responsibilities for the ASD(C3I)/CIO secretariat were specifically addressed during the DRI activities in particular DRI Directive (DRID) 17. Other DRIDs were also issued that consolidated and refined ASD(C3I)/CIO functional authorities.

<u>DRID 17: Review of OASD(C3I)/CIO</u>

Initially the Department wanted to do a massive realignment of functions of the then ASD(C3I) office to include:

- ➢ Establishment of a new ASD(I); disestablishment of ASD(C3I)
- ➢ Realignment of C3 and intelligence acquisition functions to USD(A&T)

Mr. Duane Andrews, former ASD(C3I), was asked to develop a blueprint to organize these changes.

What resulted was a reevaluation of the original direction. Mr. Andrews' report, while endorsing the strengthening of overall control over intelligence and C3, recommended that the functions not be split up. In fact, the key recommendation was to retain the ASD(C3I)/CIO secretariat and strengthen it. At the same time, the report recommended that acquisition functions, while still retained within the ASD(C3I)/CIO office, would be vetted through USD(A&T) to integrate better overall Defense investment decisions. In addition, consolidation within ASD(C3I)/CIO of a number of functions that were being done by other OSD offices, was also recommended.

RESULT: In light of the many complex interrelationships among the various systems and capabilities that make up command, control communications, computers, and intelligence, along with the overall CIO functions and Departmental responsibilities, it was decided that the ASD(C3I)/CIO secretariat would be retained and strengthened. Senior leadership recognized that 1) information superiority requires collection and integration of all forms of information (intelligence, blue force, open source, coalition, etc); 2) information needs to be turned into knowledge; 3) information needs to be secure; and 4) information is worthless unless it can be properly communicated to the consumer. The Department's leadership realized that splitting up ASD/C3I/CIO was incompatible with making Information Superiority happen, which was a recurring theme in the report. Therefore, ASD/(C3I)/CIO retained overall oversight of all those functions.

Once the decision was made to retain and strengthen the ASD(C3I)/CIO secretariat, a number of other DRIDs were issued to integrate better the Department's overall Information Superiority functions and responsibilities.

DRID 11, Reorganization of DoD Space Management Responsibilities

An aggressive review was conducted on the overall management of space activities. Results of the review included the following that strengthened the Department's oversight and management of this area:

- The space policy, space systems and architectures, space acquisition and management, and space integration functions of the former DUSD (Space) were realigned to the ASD(C3I).

- The National Security Space Architect (NSSA) was established for both Intelligence and DOD systems/capabilities. Further, a joint DOD/DCI Senior Steering Group was established to oversee/direct the work of the NSSA. ASD(C3I)/CIO is the lead for the Department and is one of the tri-chairs for the Senior Steering Group, the others being the Joint Staff's J-8 and the DCI's Deputy Director of Central Intelligence for Community Management.

NOTE: DRID 42, as a follow-up, transferred space policy functions from USD(A&T) and USD(P) to ASD(C3I)/CIO to ensure that the Department had a single focal point for all space-related functions.

DRID 31: Realignment of DoD Spectrum Management Responsibilities

Spectrum management has become increasingly more important and complex. The Department asked the Joint Staff to submit a proposal to realign duties and responsibilities in the spectrum management area that were currently being performed throughout the Department. Based on the study results

- ASD(C3I)/CIO designated a Special Assistant for Spectrum Management as the DOD focal point to carry out the policy, planning, and oversight functions associated with DOD spectrum.
- In addition, DISA established an office to coordinate joint spectrum matters and assist OASD(C3I)/CIO in conducting strategic planning.
- The Services were to co-locate their frequency management offices with the DISA office to facilitate coordination and development of joint positions. (This has been done.)

DRID 43: Defense-wide Electronic Commerce

A new program, the Joint Electronic Commerce Program, was formed under the oversight of the ASD(C3I)/CIO. This program was to foster the evolving business methodology for enterprise-wide conduct of secure business transactions via electronic means. This is to help promote more efficiency and effectiveness by leveraging the "Revolution in Business Affairs."

DRID 46: Paperless Contracting

This DRID formalized and focused paperless contracting activities under the ASD(C3I)/CIO. Increased emphasis was directed by this DRID to the CIO's authorities and responsibilities under the Clinger-Cohen Act.

Management Studies and Issues

ASD(C3I)/CIO is working on several management studies that may result in significant recommendations for consideration by the Department's senior leadership. Conclusions from these studies will be briefed as soon as they become available.

Specific studies include:

- Defense Intelligence for the 21st Century
- Defense Intelligence Infrastructure Assessment
- Re-engineered Interoperability Process
- Information Superiority Investment Strategy
- Integrated Protection Broad Area Review
- Strategic C3 Modernization
- CIO Relationships, Processes and Performance Measures
- International Mobile Communications 2000 Spectrum Studies

Completed studies include:

- Space Control Broad Area Review--Approved by the Deputy Secretary of Defense in March of 2000, this review had 26 discrete recommendations to improve space surveillance, space protection, prevention and denial. This product serves as an architecture for the future of Space Control.

- Unmanned Aerial Vehicle (UAV) Roadmap--Developed in conjunction with USD(AT&L) this document describes the current state of UAV activities in DoD, the payload priorities, the Services' forecast for the future programs and technologies. It also highlights the challenges yet to be resolved such as the integration of UAVs into the national airspace.

- Intelligence, Surveillance, Reconnaissance (ISR) Integrated Capstone Strategic Plan- Approved by ASD(C3I)/CIO in November 2000. This document defines the DoD ISR vision of an integrated and responsive capability operating in a collaborative enterprise assuring delivery of timely, relevant information for the National Command Authority and the Joint and Combined Forces.

- Model CIO Study--Study presents a composite for an ideal CIO organization addressing responsibilities relationships, core competencies, structures, processes and performance measures The study examines CIO issues and practices from industries similar to DoD.

C. EXternal process

EXECutive Key Interagency Relationships

Major Interfaces between the Office of the ASD(C3I)/CIO and the Components of the US Intelligence Community (IC), the NSC and other Federal Agencies

1. Director of Central Intelligence (DCI). ASD(C3I)/CIO interacts with the DCI in two fashions: directly with the CIA and through the Community Management Staff (CMS).

- Involvement with the CIA:
    - To ensure adequate support to military operations from various CIA activities involved in collection, analysis and production, and dissemination of intelligence products and services.
    - To receive DCI's guidance on DoD's rules of engagement for intelligence sharing with foreign governments. This determination is done through CIA.
- The largest degree of interaction is with the CMS:
    - CMS assists the DCI in IC coordination and management responsibilities for resource management; program assessment and evaluation; policy formulation; and collection management and other duties.
    - ASD(C3I)/CIO interfaces with the CMS through a variety of boards, panels, working groups and formal fora. Among these are:
        - IC Principals Committee, composed of the Directors of every Intelligence Component and the IC Deputies Committee. While OASD(C3I)/CIO is invited as an observer, it does exercise considerable influence in these fora.
        - Other important panels address Information Assurance, counterintelligence (CI), collection management, and production. Additional coordination regarding the development of the National CI Initiative – CI-21 has been ongoing with the National CI Center.

2. Defense Intelligence Agency (DIA). ASD(C3I)/CIO exercises staff supervision of the DIA through the line relationship between the ASD and the Director, DIA.

- ASD(C3I)/CIO maintains a Performance Contract with the Director DIA. This document codifies the vision and the primary goals and objectives agreed between the two principals and is reviewed quarterly.
- There are a variety of interchanges between ASD(C3I)/CIO personnel and DIA. These include:
    - Senior Intelligence Officer monthly meetings, and bi-weekly intelligence directors' breakfasts.
    - The Military Intelligence Board.
    - The semi-annual Senior Military Intelligence Officers Council which is the primary venue at which the DIA Director exercises leadership of the Service and Command intelligence organizations.
- ASD(C3I)/CIO maintains continuous contact with DIA on current CI investigations, collection efforts and analysis as they pertain to DIA.

3. National Imagery and Mapping Agency (NIMA). In addition to the contacts in (2) above, ASD(C3I)/CIO participates in the oversight of major NIMA projects, chief among them being the United States Imagery and Geospatial Service (USIGS), a multi-million effort to upgrade imagery tasking, production, and dissemination capabilities.

4. National Security Agency (NSA). In addition to the contacts in (2) above, the ASD(C3I)/CIO:

- Participates in the Expanded Community Management Review Group where the Director of NSA discusses major issues related to SIGINT with major DoD and IC stakeholders.
- Works closely with NSA's Information Systems Security Organization for the development and promulgation of technical security solutions and oversight of the Information Systems Security Program which contains the majority of the Department's Information Assurance initiatives.
- Works with NSA in their role as the National Information Security Manager. To that end, the ASD(C3I)/CIO serves as the Chairman of the National Security Telecommunications and Information System Security Committee.

5. National Reconnaissance Office (NRO). Besides the contacts in (2) above, ASD(C3I)/CIO is directly involved with the Director of NRO on special projects or major initiatives related to space-related capabilities.

6. National Security Council (NSC). The USD (Policy) or the General Council usually is the principal interlocuter with the NSC. However, ASD(C3I)/CIO interfaces with the NSC on several specific matters. These include

- Interactions on specialized matters for which the NSC staff has been assigned approval/disapproval authority on a standing basis by the NCA or by Presidential direction.
    - An example is ASD(C3I)/CIO's continuing coordination on activities in the Sensitive Reconnaissance Operations program.
    - Others include encryption policy and certain export control issues.
- Specific C3I/CIO responsibilities such as critical infrastructure protection, port security, Security Policy Board questions, counterintelligence, and information assurance questions.
- Problems referred by the Secretary of Defense to provide direct support on issues under NSC consideration.

7. State Department (DOS). ASD(C3I)/CIO interfaces with DoS on a variety of subjects including, but not limited to, intelligence support to diplomatic operations and treaty verification. ASD(C3I)/CIO also deals with State's Bureau of Intelligence and Research (I&R) on substantive issues, coordination of products, and technology transfer issues.

8. Department of Energy (DoE). ASD(C3I)/CIO has contacts with DoE on all joint investigations at national and military laboratories and in ongoing efforts to protect highly-sensitive technologies. The Security Directorate of ASD(C3I)/CIO focuses on all aspects of industrial and nuclear security issues.

9. Department of Justice (DoJ).

- The Deputy Director of the National Infrastructure Protection Center is assigned from ASD(C3I)/CIO.
- ASD(C3I)/CIO interfaces with DoJ on the status of joint FBI/DoD CI investigations and inquiries, antiterrorism initiatives, the review of espionage, computer crime and attacks on DoD information systems, other significant investigative activities, and in the development of CI-21.

10. Federal CIO Council. The ASD(C3I)/CIO is a member of the Council, a forum charged with improving federal agency practices on the design, modernization, use, sharing, and performance of information resources.

- It serves as a focal point for coordinating responses to government-wide information technology challenges and partners with other governmental councils to address issues that require multidisciplinary and multi-level concerns.
- The Council is composed of the CIOs and Deputy CIOs of the 28 largest executive agencies, as well as key officials from OMB, OSTP and other technology boards.

11. National Security Telecommunications Information Systems Security Committee (NSTISSC). The NSTISSC is authorized under National Security Council (NSC) Directive 42. The National Security Agency (NSA) performs the oversight of the NSTISSC and its various subcommittees. ASD(C3I) chairs and C3I has membership at the committee level usually represented by DASD (S&IO). The NSTISSC provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the NSTISSC Issuance System. National security systems contain classified information or:

- involves intelligence activities;
- involves cryptographic activities related to national security;
- involves command and control of military forces;
- involves equipment that is an integral part of a weapon or weapons
- system(s); or
- is critical to the direct fulfillment of military or intelligence missions (not
- including routine administrative and business applications).

Congressional

ASD(C3I)/CIO Role In The Legislative Process

Authorization: ASD(C3I)/CIO takes its lead from ASD(LA), which is chartered to interface with Members and committees regarding issues and matters of interest to the ASD(C3I)/CIO. Typically, ASD(C3I)/CIO, with full concurrence of the ASD(LA), deals directly in responding to the Intelligence oversight committees of Congress.

Intelligence Oversight: The Senate established the Senate Select Committee on Intelligence (SSCI) on 19 May 1976. The House of Representatives followed suit on 14 July 1977 by creating the House Permanent Select Committee on Intelligence (HPSCI). These committees are charged with authorizing the programs of the intelligence agencies and overseeing their activities.

Appropriations: ASD(C3I)/CIO takes its lead from USD(C), which is chartered to interface with Members and committees regarding issues and matters of interest to the ASD(C3I)/CIO. The Appropriations Committees, given their constitutional role to appropriate funds for all US Government activities, also exercise some oversight functions

The OASD(C3I) Office of Congressional Affairs serves as special assistant to the ASD for the following:

- Translating DASD issues into a comprehensive ASD(C3I)/CIO legislative strategy
- Supporting development of Congressional testimony by ASD(C3I)/CIO representatives (oral testimony, written Statements for the Record, visual displays, backup materials) on intelligence, security, CIO, or Information Superiority issues
- Reviewing Congressional marks and language
- Tracking and distributing pertinent Congressional information
- Preparing/disseminating executive summaries
- Tasking and assembling classified and unclassified appeals
- Identifying, tracking, and validating Congressionally Directed Actions
- Organizing and conducting staffer outreach programs
- Responding to ad hoc taskings and inquiries

Key Committes

A. Key Committees (Members as of 12/18/00)

Senate Appropriations Committee/Defense Subcommittee (SAC-D)

Majority

Honorable Ted Stevens
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington DC 20510-6028

Minority

Honorable Daniel K. Inouye
Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington DC 20510-6028

House Appropriations Committee/Defense Subcommittee (HAC-D)

Majority

Honorable Jerry Lewis
Chairman, Subcommittee on Defense
Committee on Appropriations
House of Representatives
Washington DC 20515-6018

Minority

Honorable John P. Murtha
Subcommittee on Defense
Committee on Appropriations
House of Representatives
Washington DC 20515-6018

Senate Armed Services Committee (SASC)

Majority

Honorable John Warner
Chairman, Committee on Armed Services
United States Senate
Washington DC 20510-6050

Minority

Honorable Carl Levin
Committee on Armed Services
United States Senate
Washington DC 20510-6050

House Armed Services Committee (HASC)

Majority

Honorable Floyd Spence
Chairman, Committee on Armed Services
House of Representatives
Washington DC 20515-6035

Minority

Honorable Ike Skelton
Committee on Armed Services
House of Representatives
Washington DC 20515-6035

Senate Select Committee on Intelligence (SSCI)

Majority

Honorable Richard Shelby
Chairman, Select Comm. on Intelligence
United States Senate
Washington, DC 20510-6475

Minority

Honorable Richard Bryan
Select Committee on Intelligence
United States Senate
Washington, DC 20510-6475

House Permanent Select Committee on Intelligence (HPSCI)

Majority

Honorable Porter J. Goss
Chairman, Permanent Select Committee
on Intelligence
House of Representatives

Minority

Honorable Nancy Pelosi
Ranking Minority Member
Permanent Select Committee on Intelligence
House of Representatives

Critical Reports

Critical Reports to Congress

Report	Directed by Committee/Conference	Description
Measurement and Signatures Intelligence (MASINT) Feasibility Study	Intelligence Authorization Conference	Directs study and report on the feasibility & utility of improving the management & organization of MASINT
CIO-related; Clinger-Cohen Implementation	Defense Appropriations Conference & Defense Authorization Conference	Directs registration & certification of info systems with CIO; report on implementation of additional Clinger-Cohen requirements; tracking of IT purchases
Tracking, Processing, Exploitation and Dissemination (TPED) Pre-acquisition effort	Intelligence Authorization; Defense Appropriations	Plus-up of $100M; Directs architectural study of TPED 2nd Phase, and an R&D funding roadmap
Intel Community Communications Architecture	Intelligence Authorization	Study and assess the Intelligence Community's communications shortfalls & make recommendations
Information Assurance (IA)	Defense Authorization	Establish IA Institute and report on implementation of the "Government Information Security Reform Act"
Network Centric Warfare (NCW)	Defense Authorization	Report on concept and implementation of NCW

A comprehensive list of Congressionally Directed Actions is available at our ASD(C3I)/CIO Web site (http://anet.c3i.osd.mil)

Legislation Issues

Pending Legislative Issues

Nortel Networks Corporation/ Siemens Business Communications Systems Switches – Nortel has complained to Senators Warner and Robb about preferential treatment being given to Siemens at 2 European installations. The issue centers around army Communications and Electronics Command (CECOM) contract requirements and subsequent award to Siemens and compliance with telecommunications standards.

Defense Security Service (DSS) Backlog – DSS backlog of outdated security clearances for both government personnel (civilian & military) and contractors has become very large (about 450,000). ASD(C3I)/CIO and DSS are working to remedy the problem.

John Deutch – What DoD did or didn't know and do. Congress, particularly the Intelligence Committees are concerned about when and how the CIA and DoD responded to knowledge that former DepSec Dep/former Director of Control Intelligence (DCI) Deutch carried and worked on classified information at home on his personal computer.

Department of Energy (DoE), Wen Ho Lee, China – The Wen Ho Lee incident has significant counter-intelligence implications for Defense as well as the rest of the national security system. There is directive language in the FY01 intelligence legislation that addresses improved security for DoE.

Security Locks (MAS Hamilton – KY Delegation) – A Kentucky company (MAS-Hamilton) makes the only federally approved security locks in the country and wants DoD to buy them until all DoD (government and industry) containers are fitted with their (the infamous) MAS-Hamilton X-07 / X-09 locks.

IT Workforce Issues - ASD (C3I)/CIO continues to work with USD(P&R) to address recruiting and retention problems associated with Information Technology specialists. ASD(C3I)/CIO has submitted a legislative proposal for the FY02 Defense Authorization Act and will continue to meet with P&R to address this issue.

Iridium – DoD awarded Iridium Satellite LLC of Arnold, MD, a $72 million contract for 2 years of unlimited airtime for 20,000 government users over the Iridium Satellite network. The contract includes an indemnification agreement. The negotiations were not fully supported by Congress and some backlash <u>may</u> result.

II Budget

A. Budget Overview

Budget Overview - Key Upcoming PPBS Events

Finalize FY02-07 President's Budget

- **November/December 00:** FY02-07 Program Budget Decisions issued.

- **January 01:** Major Budget Issues resolved

- **February 01:** Submit FY02-07 Budget to the Congress.
  - ➢ Topline information forwarded.
  - ➢ Details to follow based on final review by new Presidential Team with subsequent submission of Amended FY02-07 President's Budget.

- **March/April 01:** Send Amended FY02-07 President's Budget to the Congress.

- **March - September 01:** Congressional reviews/marks; Information from ongoing QDR may modify Budget Request.

FY03-07 Program/Budget Review Process

- **February/March to September 01:** Quadrennial Defense Review. QDR issue development/results are key basis for Program/Budget Review.

- **May 01:** Publish FY03-07 Defense Planning Guidance.

- **July/Aug 01:** Each Service/Agency submits its Program Objective Memorandum and Budget Estimate Submission to OSD for review.

- **October 01:** Program Decision Memoranda issued. This is a very short timeline when compared with the normal sequential timelines of PPBS. Accordingly, it will need to "blend" with the parallel ongoing budget review.

- October/December 01: Program Budget Decisions issued.

- **January/February 02:** Submit FY03-07 President's Budget to Congress.

Defense Intelligence Program/Budget Review: A joint program/budget review is conducted on all Defense Intelligence programs (National, Joint, and Tactical). Co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence, the process is run in parallel with the overall DOD program/budget review process The dates for program input, reviews and final decisions are similar to those shown above.

B. Budget Details

ASD/C3I FY 2001 Resources (Dollars in Millions)

C3I Mission Evaluations and Assessments Funds	47
Command Information Superiority Architectures	9
Information Superiority & Integration Support	11
CIO New Mission	14
Special Intelligence	145
National Security Space Architecture	10
Common Joint Tactical Information	16
Command and Control Research Program	2
Congressional Adds	74
Total	328

Program Narratives

C3I Mission Evaluations and Assessments Funds

Provides resources to perform studies and technical analyses of ongoing and emerging requirements in the Department's command, control, communications, computers, intelligence, reconnaissance, and surveillance (C4ISR) activities. These analyses support the management and oversight of DoD policies, principles, and guidance for C4ISR programs.

Command Information Superiority Architecture

Provides CINCs with a structured planning process to define current and objective command capabilities to provide C4ISR support to assigned missions. CISA implements the C3I goal of building a coherent global network by building on past successful operationa, systems, and technical architectures and other warfighter plans. It establishes common, coherent CINC "go to war" capabilities and identifies differences in capabilities between CINCs.

Information Superiority & Integration Support

Provides resources to plan and implement Joint and Combined end-to-end integration of Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C3ISR) and space systems to achieve information superiority. Analyses will provide the Department's vision, policy, and standards for ISR airborne and overhead sensors and ensure necessary interoperability to support strategic and tactical requirements. ISIS supports a move towards an Integrated ISR Enterprise (IIE) that is incorporated into the Global Information Grid (GIG).

CIO New Mission

Provides resources to ensure the Department's management and acquisition of information technology (IT) is in compliance with the Clinger-Cohen Act. This includes strategic planning and providing overall direction and guidance for managing information resources. Specific responsibilities include promoting the effective and efficient design and operation of all major information management processes, including work process improvements; developing, maintaining, and facilitating the implementation of an integrated IT architecture for the department; designing and implementing a process for maximizing the value and assessing and managing the risks of IT acquisitions; evaluating the performance of IT programs; and advising the SecDef on IT-related issues.

Special Intelligence

Provides resources to support compartmented programs. A more detailed briefing will be provided to the transition team separately.

National Security Space Architecture

Provides resources to support the National Security Space Architect (NSSA) program. Funds are used to integrate space system architectures, eliminate unnecessary vertical stove-piping of space programs, and achieve efficiencies in acquisition and future operations through space program integration, thereby improving space support to a variety of customers. These resources support DoD requirements only. The NSSA has secondary funding in the DCI program.

Common Joint Tactical Information

Provides resources to fund ongoing system level engineering of the existing Link 16 system for joint interoperability and the development of next generation Link 16 system, the Multifunctional Information Distribution System (MIDS). System level engineering responsibilities include Link 16 spectrum issues and Link 16 joint enhancements. Spectrum issues include system engineering, testing, maintaining necessary equipment, performing DoD internal and external coordination and platform integration/certification required to coexist and operate in the Air Force Navigation Safety frequency band

Command Control Research Program

Provides resources to support research into emerging technologies, methodologies, and theories of military command and control (C2), the application of research results to resolve the problems of C2 associated with joint and coalition operations and the optimal use of Military Department laboratory resources.

MASINT Feasibility Study (Congressional Add)

Provides resources to conduct a study of feasibility and utility of improving the management and organization of Measurement and Signature Intelligence (MASINT) including enhancing connectivity and dissemination capability for MASINT collection and analysis, developing a MASINT requirements system, establishing a data archiving capability, identifying how MASINT fits into the multi-disciple intelligence community environment, and improving doctrine and training requirements to support making MASINT available to both the IC and warfighters on a more timely basis. The Central ASINT Office is responsible for executing these funds in coordination with ASD(C3I)/CIO and the DCI.

Facilities, Infrastructure and Engineering System (FIRES) Data Capture (Congressional Add)

Provides resources to leverage existing infrastructure data, evolve focus areas, and develop platforms to centralize requirements, correlate data, and disseminate information across a universal, protected network.

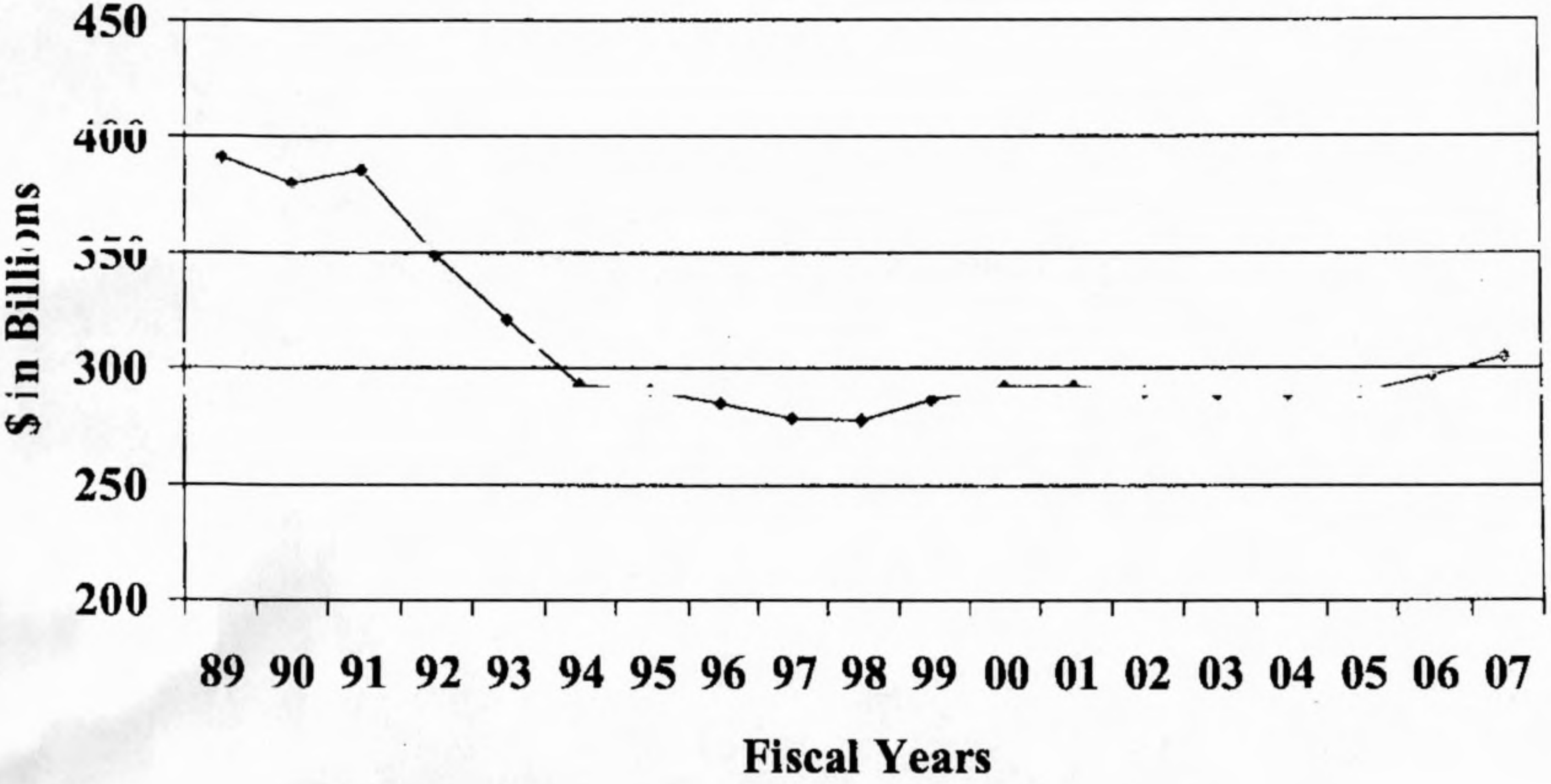
Pacific Disaster Center (Congressional Add)

Provides resources to support the Pacific Disaster Center, a federal information collection, processing, and dissemination facility to support cost-effective and efficient emergency management of natural and human induced disasters. The PDC mission is to provide information products and services to decision makers involved in protecting and preserving life, property, and infrastructure, and ensuring continuity of operations threatened by disasters.

C. Budget Trends [redacted]

UNCLASSIFIED

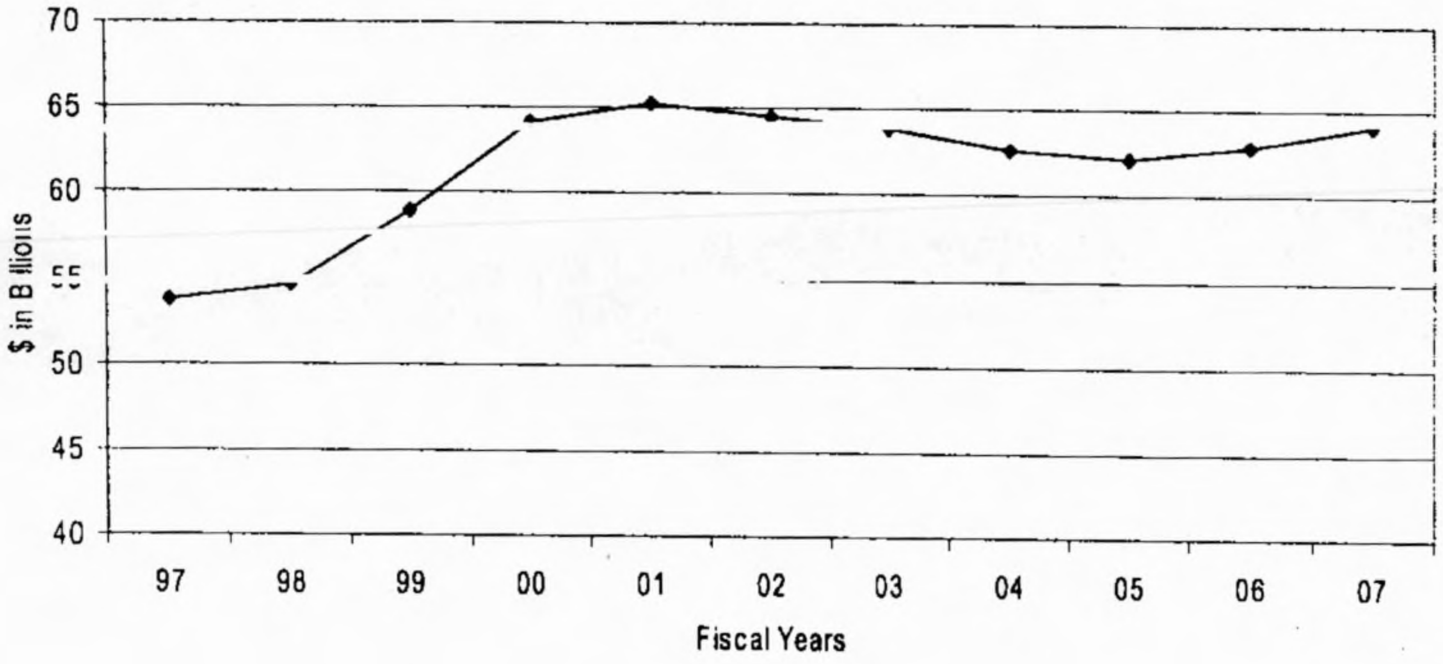
Total DoD Budget Trend
TOA in Constant FY2001 Dollars



12/19/2000 3:58 PM

UNCLASSIFIED

C3I INFORMATION SUPERIORITY PROGRAMS
Budget Trend
in Constant FY2001 Dollars



D. Budget Issues

Budget Issues

Special Navy

A very specialized capability within the Special Navy Program is programmed to cease at the end of FY 2002. No other source can provide this unique information. $250 million is required in FY01-05 to sustain this critical capability. Classified details of this subject are available.

REDSKY

Funding ($ 26 million) is needed in FY 2001 to acquire sensing and warning capability for attacks against DoD networks. Funding for FY 2002-2007 has been programmed. Classified details of this subject are available.

III Personnel

A. Statistics

ASD/(C3I)/CIO Manpower Summary

ASD(C3I)/CIO government employees – 282
ASD(C3I)/CIO is authorized an OSD government staff of 282, including both military and civilian employees. As of this writing, this authorized manpower ceiling of 282 encompasses approximately 49 employees and their positions that are in the process of being realigned from the Defense Intelligence Agency (DIA) into OASD (C3I)/CIO as OSD employees. Upon the completion of this realignment, all 282 employees will be managed and serviced under the auspices of the Washington Headquarters Services as OSD employees.

Attached Personnel – 93
ASD(C3I)/CIO has 93 approved liaison and detailee positions. The personnel attached to these positions come from the various organizations that support the mission of OASD (C3I)/CIO. These positions mainly come from: Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA), National Security Agency (NSA), National Imagery and Mapping Agency (NIMA), National Security Space Architect, National Reconnaissance Office (NRO).

Technical expertise
ASD(C3I)/CIO utilizes allocated mission funds to hire the technical expertise that cannot be located in the government and that is critically necessary to perform our missions and functions.

[redacted] B. Pers Mgmt Issues

Personnel Management Issues

Subject: Personnel Challenges to Achieving Information Superiority

Background: The human resource challenges for achieving Information Superiority have changed significantly over the last decade as a result of many factors. A robust economy, civilian sector competition for employees to fill high-technology positions, declining American public interest in public service, major changes in the Department of Defense's (DoD) missions and operational tempo, and a significant downsizing of the Department's workforce are some of the challenges. Reducing the size of the overall workforce by more than a million personnel has left in place a very different force distribution — in age, education, and skill. Managing and shaping this force to meet current and future needs in Information Superiority is a critical task, which requires new tools, authorities, and management attention.

Discussion: Recruiting, training, and retaining (motivating) appropriate personnel is essential to building and sustaining the Information Superiority workforce. There are tremendous challenges in maintaining any civilian and military workforce today, including the active and reserve components. Attracting young, talented individuals into the Information Superiority-related fields is difficult. This includes fields such as Engineering Specialists, Computer Specialists, Intelligence Officers, Weapons Specialists, Program Managers, Acquisition Officers, and much more. Competition from the private sector for expertise needed to achieve Information Superiority is acute. Also, there is a growing shortage of quality mangers in place to fill the career positions that will become available as the aging civilian force becomes eligible to retire in large numbers in the next few years. Many of those retiring will take with them highly specialized and technical skills — ones not quickly or easily replaced — and they represent a significant portion of the civilian leadership today. In addition, senior civilian positions now stay vacant for longer and longer periods because of the reluctance of highly qualified individuals to be subjected to the political appointment process and the restrictions imposed on returning to their private sector careers.

As we move toward the 21st century, it has become increasingly important for the DoD to recruit and retain information technology (IT) professionals with the skills and competencies needed to meet new technology challenges and remain competitive with the private sector. The Federal CIO Council has recognized that recruiting and retaining IT professionals are problems for all Federal agencies. In June 1999, the Council's IT Workforce Committee reported that the demand for highly skilled IT workers was growing at an extraordinary pace, while employers around the country-including the Federal government-struggled to meet their needs for these workers. As of today, more than a year later, the situation has not changed.

The Human Resource challenges facing the DoD intelligence Community (IC) are a subset of the broader "intellectual capital" crisis negatively impacting the DoD in particular and the Federal Government workforce in a more general sense. The rapidly expanding and robust economy; increased civilian sector competition for employees to fill high-technology, information age positions -- especially within the Metropolitan Washington D.C. area; the declining interest in public service; significant post-Cold War changes to the DoD's missions leading unexpectedly to a greatly increased operational tempo; as well as significant post-Cold

War downsizing of the DoD's workforce -- reducing the size of the DoD workforce by more than a million people -- has made the DoD IC less competitive in today's modem marketplace for talent. In addition, the needs for many other languages have been either ignored or given low priority. With missions including peacekeeping, humanitarian aid, nation-building and training of foreign military personnel, more than 40,000 U.S troops are or have been stationed in more than 110 nations (excluding NATO countries and Japan) since 1991, including every nation in Latin America, all but two of the fifteen successor states to the USSR, some forty nations in Africa, and throughout South and Southeast Asia. More than 140 languages are spoken in these nations. The ability to communicate with military forces of other nations in a coalition, the ability to communicate with the people in a disaster stricken country, the ability to act as peace-keeper in situations such as Bosnia and Kosovo, demands higher skills in listening, understanding, and speaking. Cultural awareness is essential in such operations, also, and that awareness and understanding is facilitated by sound knowledge of the language.

Recommendation At the Federal Government level, it is recommended that we attempt to galvanize support and initiate action at the Office of Personnel Management (OPM) for the following efforts:

- Identify priority areas (skills/tools) for an Information Superiority workforce
- Plan for outreach (recruitment in the public sector) targeting personnel at the above identified skills
- Building on these previous efforts, develop a Department HR Plan that specifically identifies needs, strategies and policies that are required to shape a quality and skilled workforce essential for Information Superiority
- Develop training for the 21st century for an Information Superiority workforce
- Develop cross-Service programs to capture and leverage all ideas/efforts to enhance Information Superiority, and to motivate the workforce and imbue it with the sense that it is part of a progressive and over-arching enterprise.

As DoD develops strategies for recruiting and retaining IT professionals, the Department may need to take advantage of human resource management flexibilities and resources are available to help address the recruiting and retention problems facing IT managers. OPM has compiled a list of human resource management approaches and tools that Federal agencies may use in designing IT recruitment and retention strategies and in resolving current staffing problems. The Federal CIO Council has posted the list on its website (www.cio.gov). The list includes:

- Advance payments (up to four weeks' pay) for new employees.
- Recruitment and relocation bonuses (up to 25 percent of annual base pay).
- Retention allowances (up to 25 percent of base pay).
- Paying for Training and Education (includes tuition).

IV policy issues

A. Dev Process

Overview of the Policy Development Process

The ASD(C3I)/CIO participates in many policy development activities. These can be broken down into Executive Branch Legislative Branch and international activities.

Executive Branch

- DoD. Within DoD, the ASD(C3I)/CIO's policy-related actions range from support to NCA decision-makers in contingency operations (such as Kosovo), to the development and exercise of policy, oversight and guidance in matters such as information assurance, critical infrastructure protection, network governance, acquisition of C3ISR and IT-related systems, space policy, management of the IT workforce, intelligence issues, security, counterintelligence and information operations, electronic business and R&D objectives.

  - Policies developed through internal DoD coordination may be codified through the Instructions and Directives process, or through Guidance and Policy Memoranda (G&PM). The latter have the force of law but are only enforceable for a period of 180 days and expire at the end of that period. To remain in force for a longer period requires a more formal coordination effort known as the SD 106 process (for the coordination form of the same name used for routing the document).

  - The SD-106 process usually takes about 12 months – which is why a G&PM is customarily used as a gap-filling mechanism to facilitate prompt implementation. Examples of this approach used in are the Global Information Grid (GIG) policy document suite. Customarily we share these policy initiatives with the Director of Central Intelligence (DCI) s staff as a professional courtesy although they are not formal participants in the process.

- Intelligence Community (IC) There is an extensive series of interactions with the IC, ranging from discussions over the supervision of the defense-related intelligence agencies (DIA, NSA, NRO and NIMA), to budget-related issues (which often are driven by policy questions between the SecDef and DCI), to recommendations to the SecDef concerning sensitive intelligence activities.

  - The National Security Act of 1947 (as amended) and the Executive Order 12333 designate the DCI as the formal, titular head of US Intelligence. In this role, the DCI can publish policy for the US Intelligence Community, which includes the Defense Intelligence components. While not directly responsible for the daily management, direction or control of Defense Intelligence components, the DCI does have considerable authority over many aspects of their activites.
  - One vehicle the DCI uses to establish policy is the DCI Directive (DCID), which is similar to a DoD Directive and also carries the power of law. DCID's are coordinated by the Community Management Staff (CMS) with DoD, CIA and the intelligence activities of the Depts of State, Energy, and Justice, and the FBI. Recent DCIDs have addressed intelligence sharing agreements with foreign nations, protection of sources and methods, and Warning, Critical Communications, and Emergency Planning.

- Broad Inter-agency. Although USD(Policy) has the lead for most activities broader inter-agency fora, the ASD(C3I)/CIO speaks for Department in the NSC-led Critical Infrastructure Coordination Group and Cyber-Incident Steering Group, and the chairs the National Security Telecommunications Information Systems Security Committee (NSTISSC). Inter-agency activities may be used to tee up issues for resolution at the Deputies or Principals Committee level. They also may lead to the development of Executive Orders (E.O.) or Presidential Decision Directives (PDD). PDDs usually are preceded by a Presidential Review Directive (PRD), which typically is a study in preparation for a PDD A classified PRD now is in progress to help clarify elements of computer network operations for the transition.

Legislative Branch

- ASD(C3I)/CIO takes its lead from ASD(Legislative Affairs) in dealing with the Authorizing Committees, and from Comptroller in dealing with the appropriators. However, ASD(C3I)/CIO representatives frequently are called to testify on intelligence, security, CIO, or Information Superiority issues.
  - A number of significant policy issues have arisen out of Section 119 of title 10 that addresses Special Access Program (SAP) oversight and reporting. ASD(C3I)/CIO supports the Special Access Program Coordination Office (SAPCO) in USD(AT&L) on many Congressional actions
  - Several legislative issues pending at this time have been highlighted in the legislative issues relations section.

International Activities

- USD(Policy) and the State Department have the lead in international negotiations, and the DCI is charged with international intelligence cooperation. However, the ASD(C3I)/CIO serves as the US member on the NATO C3 Board, and a number of bi-lateral and multi-lateral fora. Recent international issues have included encryption policy, export control reform, and coalition information sharing.

B. Major Issues

Major Policy Issues

DoD is committed to taking full advantage of opportunities provided by the information age's concepts and technologies. The synergy resulting from the consolidation of Information Superiority and Chief Information Officer (CIO) functions under the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) continues to yield significant technical, operational, and financial benefits and have the potential to yield more. The United States currently enjoys a superior information position over potential adversaries by virtue of its ability to collect, process, protect, and distribute relevant and accurate information in a timely manner while denying this capability to adversaries. However, one's dependence on information also creates vulnerabilities that adversaries can exploit. Moreover, there are significant organizational and statutory improvements that are impeding the Department's abilities to take full advantage of this potential.

Bottom Line: All future military concepts and operations are predicated on successful implementation of information superiority. Without significant leadership attention to Information superiority U.S. Forces and DoD transformation are at risk.

The Problem: Despite significant accomplishments to date, our networks and infrastructures are vulnerable and fragile. We are unable to provide the Information Superiority needed to support the warfighter today, to support emerging operational concepts that are resulting from the Revolution in Military Affairs and to enable business process improvements and re-engineering resulting from the Revolution in Business Affairs.

Why?: The program of record is not delivering the needed information superiority capabilities soon enough. We have fragmented authorities and stove-piped processes and our polices, processes, personnel and technology and materiel are not aligned properly to achieve information superiority.

What Needs To Be Done?: There is no single solution to fix this problem. However a number of actions have been initiated and need to be sustained and even accelerated to mitigate this issue.

They include:

- Implement an effective program for establishing information assurance and critical information protection
- Build a coherent, secure, interoperable global network (the Global Information Grid)
- Achieve end to end C3ISR integration
- Promote the development of a knowledge-based workforce
- Strengthen Defense Intelligence to ensure it meets the needs of the 21st Century for warfighter and policy makers.
- Strengthen information operations, security and counterintelligence
- Promote electronic commerce and business process change
- Foster development of an advanced technology plan for information superiority

How?: Within the Department, the ASD(C3I)/CIO, the USD(AT&L), and the USD(Comptroller)/CFO can serve as powerful agents to affect changes. Addressing CIO authorities to cut across stovepipes, accelerating reforms to create a more nimble, responsive acquisition and logistics system, foster CIO-CFO partnerships to promote business process changes can be powerful tools that should be encouraged.