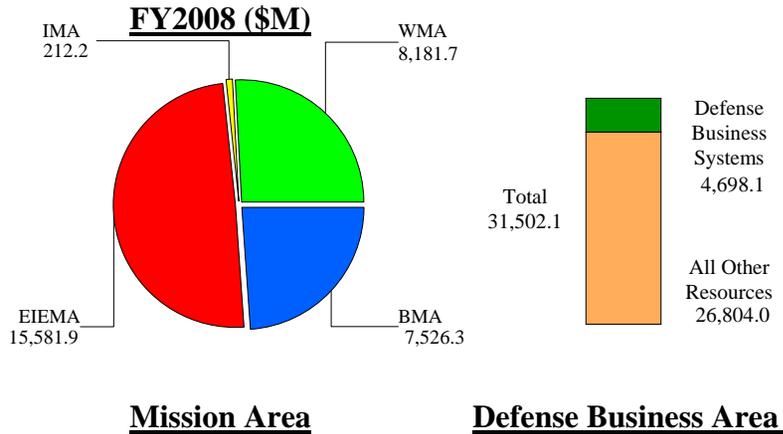


**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**



FY07/08PB Comparison (\$M)

	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>
PB FY2007:	\$ 30,870.6	\$ 31,626.8	\$ 31,958.2
PB FY2008:	\$ 30,479.0	\$ 31,502.1	\$ 32,005.4
Delta:	\$ -391.6	\$ -124.7	\$ 47.2

Explain:

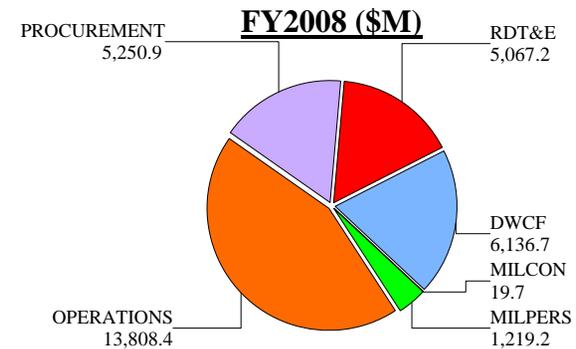
The deltas reflected between the Department of Defense FY2007 IT Budget Submission and its FY2008 IT Budget Submission are insignificant at the top-line level, less than 1.3% in FY2007 and less than .4% in FY2008. Details to changes at the Service, DoD Agency, and DoD Activities can be found through-out this submission.

FY07 to FY08 Comparison (\$M)

	<u>FY2007</u>	<u>FY2008</u>	<u>Delta</u>
PB FY2008:	\$ 30,479.0	\$ 31,502.1	\$ 1,023.1

Explain:

The growth reflected in the Department of Defense FY2007 and its FY2008 IT Budget is \$1.023B (3.4%) and can mostly be attributed to inflation at the top-line level. Details to changes at the Service, DoD Agency, and DoD Activities can be found through-out this submission.



APPROPRIATION

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY MISSION AREA (DOLLARS IN MILLIONS)			
MISSION AREA	FY2007	FY2008	FY2009
BUSINESS (BMA)	\$ 7,282.68	\$ 7,526.27	\$ 7,672.67
ENTERPRISE INFORMATION ENVIRONMENT (EIEMA)	\$15,165.90	\$15,581.91	\$15,993.13
DEFENSE INTELLIGENCE (IMA)	\$ 182.54	\$ 212.19	\$ 179.75
WARFIGHTING (WMA)	\$ 7,847.87	\$ 8,181.69	\$ 8,159.84
DOD TOTALS	\$ 30,478.99	\$ 31,502.06	\$ 32,005.39

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

DoD MISSION AREAS													
Business Mission Area (BMA)					Warfighting Mission Area (WMA)					Defense Intelligence Mission Area (DIMA)			
Governance via DBSMC					Governance via JROC					Governance TBD			
<i>Weapon System Lifecycle Management</i>	<i>Material Supply and Service Management</i>	<i>Real Property & Installation Lifecycle Management</i>	<i>Human Resource Management</i>	<i>Financial Management</i>	<i>Focused Logistics</i>	<i>Battlespace Awareness</i>	<i>Force Application</i>	<i>Force Protection</i>	<i>Net-Centric</i>	<i>Force Management</i>	<i>Joint Training</i>	<i>Command & Control</i>	Domains TBD
Enterprise Information Environment Mission Area (EIEMA)													
Governance via EIEMA IRB													
Information Assurance													
Communications				Computing Infrastructure				Core Enterprise Services					
Cross-Cutting & Interdependent Domains													

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

**DoD INFORMATION TECHNOLOGY RESOURCES
BY DEPARTMENT
(DOLLARS IN MILLIONS)**

	FY2007	FY2008	FY2009
DEPARTMENT OF ARMY	\$ 6,618.16	\$ 7,408.61	\$ 7,586.31
DEPARTMENT OF NAVY	\$ 6,595.97	\$ 6,479.97	\$ 5,962.24
DEPARTMENT OF AIR FORCE	\$ 6,897.32	\$ 7,111.73	\$ 7,736.97
DEFENSE WIDE ACTIVITIES	\$10,367.54	\$10,501.74	\$10,719.88
DOD TOTALS	\$30,478.99	\$31,502.05	\$32,005.40

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

OVERVIEW

The Power of Information

Access – Share – Collaborate

Where it's needed, When it's needed, To those who need it most

Defense transformation is a key element of the Department's Defense Strategy established by the Secretary to meet the challenges of the dangerous and uncertain security environment of the 21st Century. This transformation is intended to make dramatic changes in how the military fights and how the Department does business. The Secretary of Defense has identified six critical operational goals that provide the focus for the Department's transformation efforts:

- Protect critical bases and defeat chemical, biological, radiological, and nuclear weapons
- Project and sustain forces in anti-access environment
- Deny enemies sanctuary
- **Leverage information technology**
- **Assure information systems** and conduct information operations
- Enhance space capabilities

Transformation hinges on the recognition that information is our greatest source of power. Information can be leveraged to allow decision makers at all levels to **make better decisions faster** and **act sooner**. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it is at the heart of the capability needed to **conduct Network-Centric Operations (NCO)**.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

Information Age Transformation

The Department is engaged in an aggressive plan to achieve information superiority by providing Internet-like capabilities throughout the DoD, thus making a broader menu of information accessible which is independent of time, place and organization. Information is essential to military operations. The DoD Chief Information Officer (CIO) has established and directed initiatives to ensure that the key elements of Net-Centric Operations are in place to support the military mission and **enable information sharing**. Additionally, the DoD CIO has established operational and organizational changes inherent in military and business transformation. Transforming to Net-Centric Operations requires people, processes, and technology to work together to enable timely **access** to information, **sharing** of information, and **collaboration** among those involved. Instead of “pushing information out” based on individually engineered and predetermined interfaces, Net-Centricity ensures that a user at any level can both “take what he needs” and “contribute what he knows.”

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**



Transform America's national security institutions to meet the challenges and opportunities of the 21st century
The National Security Strategy of the United States of America (2006)



Information Environment	Net-Centric Data Strategy	Enterprise Service Oriented Architecture	End-to-End Information Assurance (IA)
<i>Vision - Deliver the Power of Information - An agile enterprise empowered by access to and sharing of timely and trusted information</i>	<i>Vision - A flexible and agile Net-Centric, environment of "many-to-many" exchanges and effective decisions</i>	<i>Vision - A Service-Oriented Architecture that is open, output focused, and independent of location and system-ware</i>	<i>Vision - Dynamic IA in support of Net-Centric Operations</i>
<i>Mission - Enable Net-Centric Operations - Lead the Information Age transformation that enhances the DoD's efficiency and effectiveness</i>	<i>Mission - Implement a data-centric strategy allowing access to and sharing of information</i>	<i>Mission - Establish easy-to-use services to access, share, collaborate</i>	<i>Mission - Assure DoD's information, information systems, and information infrastructure</i>
<p>Major DoD Investments and Initiatives</p> <p><u>Transport</u></p> <ul style="list-style-type: none"> - Global Information Grid Bandwidth Expansion (GIG-BE) - Transformational Satellite (TSAT) - Joint Tactical Radio System (JTRS) - Teleports - Spectrum <p><u>Services</u></p> <ul style="list-style-type: none"> - Net-Centric Enterprise Services (NCES) <p><u>Security</u></p> <ul style="list-style-type: none"> - Information Assurance (IA) Solutions <p><u>Execution</u></p> <ul style="list-style-type: none"> - Data Strategy/Communities of Interest (COI) - NetOps/Management <p>Enterprise Wide Systems Engineering (EW SE)</p> <ul style="list-style-type: none"> ▪ Defines end-to-end, functional, performance, and standards baseline ▪ Requires enterprise-level decision making ▪ Builds consensus to develop technical solutions 	<p>Data Strategy Foundation</p> <ul style="list-style-type: none"> ▪ Ensures data are visible, accessible, and understandable ▪ Accelerates decision making by having data where needed and when needed ▪ Accommodates known and unanticipated users ▪ "Tags" data (intelligence/non-intelligence, raw/processed) with metadata to enable discovery ▪ Requires data and services registries to describe, post, and store ▪ Posts data to shared spaces for users to access based on identity and role ▪ Organizes around Communities of Interest (COIs) using a shared vocabulary to exchange information 	<p>Enterprise Services Overview</p> <ul style="list-style-type: none"> ▪ Messaging - Ability to exchange information among users or applications ▪ Discovery - Processes to find information content or services ▪ Mediation - Software to help broker, translate, aggregate, fuse, or integrate data/metadata ▪ Collaboration - Allows users to work together and jointly use selected capabilities on the network ▪ User Assistant - Automated "help" capabilities ▪ Information Assurance - Capabilities that provide confidentiality, integrity, availability, authorization, and assurance for information, users, applications, and networks ▪ Storage - Physical and virtual places to host data on the network ▪ Application - Infrastructure to host and organize distributed on-line processing capabilities ▪ Enterprise Systems Management (ESM) - End-to-end GIG performance monitoring, configuration management, and problem detection 	<p>IA Strategy Framework</p> <ul style="list-style-type: none"> ▪ Protect Information <ul style="list-style-type: none"> - Data protection requirements - Protection mechanisms - Robust mechanisms ▪ Defend Systems and Networks <ul style="list-style-type: none"> - Engineer defenses - React and respond - Assess and evaluate activity ▪ Provide Situational Awareness/IA C2 <ul style="list-style-type: none"> - Integrated operational picture - Coordinate IA ops and decisions - Evaluate collaboration ▪ Transform and Enable IA Capabilities <ul style="list-style-type: none"> - Ensure IA integration into programs - Dynamic IA capabilities - Improve strategic decision-making - Information sharing ▪ Create an IA Empowered Workforce <ul style="list-style-type: none"> - Standardize baseline skills - Enhance IA skill levels - Provide trained/skilled personnel - Infuse IA into other disciplines
<i>Better Decisions Faster</i>	<i>Common Data Registry</i>	<i>User-Oriented Services</i>	<i>Trusted, Dependable Data</i>

The Department of Defense will significantly enhance military capabilities through Net-Centric Operations, a solid Net-Centric Data Strategy, Enterprise Services, and End-to-End Information Assurance.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Net Centric Data Strategy

The **Net-Centric Data Strategy** focuses on data, rather than on the proprietary applications and programs that manipulate data. Those at the source of the data will be required to make it easy to find and use. It must be **visible, accessible** and **understandable**. A key element in the Net-Centric Data Strategy is the organization and operation of **Communities of Interest (COI)**. COI's are collaborative groups of users who have a shared vocabulary to exchange information. Data characteristics and content will be **"tagged"** in an agreed-to manner. The communities will range from pre-established groups with on-going arrangements, to **Unanticipated Users** and non-traditional partnerships that develop on an ad hoc basis. Individual users will determine and display content based on their specific needs, **User Defined Operating Pictures (UDOPs)**, rather than in rigid or pre-determined formats.

Enterprise Service Oriented Architecture

The Enterprise Service Oriented Architecture is open, output focused and independent of location and system-ware. The Department is establishing easy-to-use services to access, share, and collaborate by providing methods to exchange information among users or applications; discover information or services; provide data/metadata mediation; utilize selected capabilities on the network; host data in physical and virtual places; and provide end-to-end Global Information Grid (GIG) monitoring, configuration management and problem detection.

End-to-End Information Assurance

Information Assurance (IA), the greatest Enterprise challenge, is the basis for **trust**: trust in networks availability, the participants' identities, and the data's dependability and integrity. Today firewalls and software patches attempt to keep intruders out and data safe. Tomorrow's assured information will require that the individual data be secured throughout its useful lifespan. The Department is striving to provide dynamic IA to support Net-Centric Operations by assuring DoD's information, information systems, and information infrastructures meet the IA Strategy Framework.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Key Elements of Information Age Transformation

Global Information Grid (GIG):

The GIG collects, processes, stores, and manages Enterprise data and will enable Net-Centric Operations. The Net-Centric GIG (NC GIG) is not just a technological backbone. It includes: **people, process, and technology**. The NC GIG enables **“information on demand.”** The NC GIG is not a system, just as the worldwide web is not a system. The NC GIG establishes the conceptual framework for the “to-be” environment for DOD that will provide information and communication services vital to the effective conduct of DOD activities from warfighting to business. As an entity, the NC GIG is comprised of many systems that interoperate to enable information access and information sharing. In order to support the interoperability, the GIG also provides the documentation of the vision, an enterprise level “blueprint”. The vision is simple: **“Deliver the Power of Information.”** We want to enable and empower people throughout the network, including the tactical edge.

What we seek is:

- An agile, robust, interoperable and collaborative DoD,
- where warfighters, business and intelligence users all share knowledge
- on a secure, dependable and global network
- that enables excellent decision-making, effective operations and network-centric transformation.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

Internet Protocol Version 6 (IPv6)

The Department has also begun a critical transition effort to address the next generation of Internet Protocol requirements. The IPv6 transition office continues under the direction of the ASD(NII)/DoD CIO with active Joint Staff and Service participation. This office has begun the planning and integration activities necessary to take full advantage of the expanded capabilities available with IPv6. Internet Protocol (IP) is the foundation of interoperability across DoD's Global Information Grid (GIG). IPv6 facilitates achieving net-centric operations by interconnecting an increasingly mobile, wireless set of sensors, platforms, facilities, people and information on an end-to-end basis. The DoD transition to IPv6 is expected to; a) minimize later transition costs by beginning to buy IPv6 capabilities now, b) address Enterprise issues early via large scale pilot implementations, c) execute an aggressive but thoughtful end to end transition, d) protect interoperability and security during transition, and e) enable an integrated, timely IPv6 transition.

Defense Business Systems

The National Defense Authorizations Act (NDAA) of 2005 prescribed the establishment of Investment Review Boards (IRB) and the Defense Business System Management Committee (DBSMC) to certify and approve defense business system modernization/enhancement investments over \$1 million and to review all business system investments at least annually. In order to ensure compliance with the NDAA and to create strategic alignment between the Department's mission, goals and objectives and its business processes and systems, the Secretary of Defense established the following Core Business Mission (CBM) strategic capabilities and assigned responsibility for implementing these capabilities to the following Principal Staff Assistants:

- Financial Management (FM) – Under Secretary of Defense, Comptroller
- Human Resource Management (HRM) – Under Secretary of Defense, Personnel & Readiness
- Real Property and Installations Lifecycle Management (RPILM) - Under Secretary of Defense, Acquisition, Technology and Logistics
- Weapon System Lifecycle Management (WSLM) - Under Secretary of Defense, Acquisition, Technology and Logistics
- Material Supply and Service Management (MSSM) - Under Secretary of Defense, Acquisition, Technology and Logistics

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

In October 2005 the Deputy Secretary of Defense established the Business Transformation Agency (BTA) which focuses on advancing enterprise-wide business transformation. The mission of the BTA is to transform business operations to achieve improved warfighter support while enabling financial accountability across the Department of Defense (DoD). The Department's business transformation effort will enable the DoD to better support its ultimate customer—the warfighter—while providing tangible benefits to its entire stakeholder community. Some of the drivers of transformation include: support for joint warfighting capability; better information for strategic investment decisions; reduced cost of business operations; and improved stewardship to the American people. The critical success factors for achieving business transformation within the defense environment differ little from those of any large-scale business operation. These success factors (or guiding principles) include: senior leadership engagement, a unifying framework—core business mission alignment to warfighter capability, end-to-end business process improvement; proper alignment of authority and accountability; ongoing component engagement; and delivering measurable results.

Global War on Terrorism (GWOT)

The Department of Defense (DoD) IT budget includes critical command and control, information assurance, and direct warfighting support systems, as well as IT funding to implement key combat support functions necessary to win the GWOT. Service and Defense-wide key activities are discussed in more detail within their individual overviews in Section II.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Portfolio Management

On October 5, 2005 Deputy Secretary of Defense (DEPSECDEF) issued DoD Directive 8115.01 - Information Technology Portfolio Management. In addition, on October 30, 2006, the ASD(NII)/DoD CIO issued DoD Instruction 8115.02 - Information Technology Portfolio Management Implementation. The purpose of these policies is to establish and implement policy and assign responsibilities for the management of DoD information technology (IT) investments as portfolios that focus on improving DoD capabilities and mission outcomes. Keeping with policies, the DoD will publish its IT Budget Estimate Summary's and Component Overview's by DoD Mission Area for Fiscal Year (FY) 2008 and beyond (Past submissions were published by Global Information Grid (GIG) categories).

The DoD's Enterprise Portfolio is divided into Mission Area Portfolios, which are defined as Warfighting (WMA), Business (BMA), DoD portion of Intelligence (DIMA), and Enterprise Information Environment (EIEMA). Mission Area portfolios are divided into sub-portfolios (e.g., domains or capability areas) that represent common collections of related, or highly dependent, information capabilities and services. Portfolios are used to support each of the DoD's decision support systems including: the Joint Capabilities Integration and Development System (JCIDS); the Planning, Programming Budgeting, and Execution System (PPBE); and the Defense Acquisition System. Mission Areas provide portfolio recommendations to the appropriate officials for consideration in the Department's decision support systems.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

Warfighting Mission Area (WMA)

The Deputy Secretary of Defense tasked the Chairman of the Joint Chiefs of Staff (CJCS) to lead the Warfighting Mission Area. DODD 8115.01, 10 Oct 05, establishes policy and assigns responsibility to the CJCS for the management of DoD IT investments as portfolios. Additionally, the DOD 8115 Series directs the CJCS to use WMA IT Portfolio Management to influence the Joint Capability Integration and Development System (JCIDS), the PPBE process, and the Defense Acquisition System (DAS), through the appropriate policy instructions. One of the published objectives in the October 2006 Joint C4 Systems Campaign Plan is to “Manage the WMA IT portfolio investment analysis to provide prioritization and integration recommendations to the capabilities, acquisition and budget process decision makers.” CJCSI 8410.01 is Joint Staff policy for the execution of the Chairman’s Warfighting Mission Area IT PFM responsibilities. The CJCS has assigned responsibilities to IT domain owners within the Joint Staff directorates to accomplish IT Portfolio Management. The CJCS also tasked the IT domain owners to promote Net-Centric data sharing and effectively enable Communities of Interest (COIs) by providing oversight and guidance to their COIs in accordance with DODD 8320.2, Data Sharing in a Net-Centric Department of Defense. The WMA IT Domain Owner is the primary group responsible for accomplishing WMA IT Portfolio Management. The Directorate for Command, Control, Communication, and Computer (C-4) System, (J-6), integrates and manages the WMA IT portfolio management efforts.

Leveraging existing governance forums, the CJCS created eight WMA IT domains, each with an Information Technology/National Security System portfolio. The eight WMA IT domains are Net-Centric, Command and Control, Battlespace Awareness, Focused Logistics, Force Application, Force Protection, Joint Training, and Force Management. The eight WMA IT domains are aligned with the Department’s Functional Capabilities Board (FCB) construct. The Director for Command, Control & Communications (DJ6) was designated as the WMA IT Integrator responsible for integrating IT and National Security System (NSS) systems across all warfighting domains and coordinating with other mission area and DoD PFM governance forums. The Joint Requirements Oversight Council and its subordinate Joint Capabilities Board (JCB) perform governance and oversight of the WMA IT domains.

IT Portfolio Management benefits the WMA Domain in the following ways:

- Improves overall military mission effectiveness through improved IT and National Security System management decisions.
- Establishes an IT/NSS repository providing a single location for information and reducing the need for IT/NSS data calls.
- Minimizes programmatic, technical, and operational risks by choosing the best programs, systems, and initiatives.
- Reduces capability duplication and improves efficiency and cost effectiveness.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Business Mission Area (BMA)

In 2005, the Deputy Secretary of Defense (DEPSECDEF) directed the establishment of the Business Transformation Agency (BTA) as the entity responsible for executing Enterprise-level business transformation. Through a governance structure of tiered accountability, the Defense Business Systems Management Committee (DBSMC) manages the Enterprise-level requirements, while each component manages its own unique mission support requirements.

The FY 2005 NDAA states that funds may not be obligated for a Defense Business System modernization in excess of \$1M, unless the approval authority for the system certifies to the DBSMC that the system is in compliance with the enterprise architecture, provides a critical national security capability, or is necessary to prevent a significant adverse effect on another project that provides an essential capability.

The FY 2005 NDAA also established an investment management governance structure that reports to the DEPSECDEF through the DBSMC using established and chartered Investment Review Boards (IRBs). These IRBs are the mechanisms that each Certification Authority (CA) uses to provide oversight of the investment review process for business systems supporting activities under their designated area of responsibility. These IRBs are:

- Financial Management – chaired by USD(C)
- Weapons Systems Life Cycle Management and Materiel Supply & Services Management – chaired by USD(AT&L)
- Real Property & Installations Life Cycle Management – chaired by USD(AT&L)
- Human Resources Management – chaired by USD(P&R)

The IRB process ensures that new systems and existing systems under modernization are compliant with the Business Enterprise Architecture (BEA). The BEA is the enterprise architecture for the DoD's business information infrastructure and includes processes, data, data standards, business rules, operating requirements, information exchanges, and the depiction of policies and procedures. The BEA provides foundational standards for data and IT interoperability, and creates a blueprint to guide and constrain business system investments.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

The Business Mission Area (BMA) uses a tiered accountability approach to investment management, categorizing each business system into one of four tiers. Tier 1 includes all Major Automated Information System (MAIS) programs with the designation of ACAT 1A, 1AM, or 1D. Tier 2 includes all non-MAIS programs with an investment of \$10M or more. Tier 3 includes all non-MAIS programs with an investment between \$1M and \$10M. Tier 4 includes all other non-MAIS programs. All development and/or modernization efforts falling within Tiers 1-3 require IRB review, CA certification, and DBSMC approval.

Objectives of the BMA: The overall objective of the BMA is to ensure that the right capabilities, resources, and materiel are delivered rapidly to warfighters. This is done by employing a holistic, investment management approach, utilizing an investment management framework. Defense Business Transformation is driven by four strategic objectives that help shape overall priorities and serve as checkpoints around which to assess the efficacy of our transformation efforts.

These four objectives are:

1. Provide support for the joint warfighter – Joint military requirements are driving the need for greater commonality and integration of business and financial operations.
2. Enable rapid access to information for strategic decisions – To make sound and timely decisions, senior DoD leadership requires deeper insight into the Department’s business operations. At the Enterprise level, DoD has identified and focused its transformation efforts on six strategic Business Enterprise Priorities, all of which make critical business information more visible and accessible. This visibility will enable decision makers to create a linkage between strategy-based outcomes and the performance of operations, create transparency of data across organizational lines, and begin to identify performance metrics that can roll up to the Enterprise level.
3. Reduce the cost of business operations – Defense business operations are being streamlined so that DoD can more effectively deliver warfighting capabilities, contend with growing pressures on resources, and benefit from economies of scale. Accordingly, the Department is focusing its investment management on the total investment needed to achieve specific Business Capability improvements. DoD is investigating a new process, called the Business Capability Lifecycle (BCL), to accelerate the acquisition process for business systems which will allow the Department to respond to emerging technology, make better decisions faster about how to manage investments, and deliver Business Capability improvements faster.
4. Improved financial stewardship to the American people – The Department recognizes its responsibility to the American people to manage financial and human resources wisely. The BMA supports the DoD’s Financial Improvement and Audit Readiness (FIAR) Plan for achieving an unqualified audit opinion.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

Defense Business Systems: The term “defense business system” means an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. Refer to Component summaries for a detailed listing of defense business systems.

Information Assurance Activities: Information assurance is a system level activity, and is conducted by the components. Following the philosophy of tiered accountability, information assurance is not explicitly addressed at the BMA portfolio level. Refer to Component summaries of systems for a detailed listing of information assurance activities.

Major Accomplishments: As of the end of FY06, 274 systems successfully navigated the IRB/DBSMC approval process. By doing so, these critical business systems effectively certified their compliance to the architecture, and were given an appropriate level of review by senior leadership.

The BMA also implemented a new risk-based approach, called the Enterprise Risk Assessment Methodology (ERAM), designed to work collaboratively with the system developers to help business Major Automated Information Systems deliver business capabilities rapidly, at a reduced cost, by identifying program vulnerabilities and providing mitigation solutions. The findings from the first three tests cases of the ERAM led to the development of the BCL process discussed below.

Major Planned Activities: The BMA is developing a new flexible acquisition oversight model – the BCL – that allows programs to customize the content and analysis structure to the needs of the problem they are solving within an agile governance structure. Through a disciplined process of analysis and review, the BCL will provide the problem definition, solution analysis, program justification and acquisition oversight model that addresses known issues with delivering needed business capabilities rapidly and at reduced cost and risk. This approach will also allow for the continued identification and resolution of additional root cause delivery issues.

In the coming months, the BMA will be applying the BCL methodology to MAIS programs. This will accelerate the acquisition process for business systems and allow the Department to respond to emerging technology, make better informed decisions about how to manage investments, and deliver business capability improvements faster.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Global Information Grid (GIG) / Net-Centricity: The IRB/DBSMC certification and approval process requires that a business system be compliant with the overarching BEA. Since the BEA was developed using the GIG as an underpinning assumption, a system's compliance with the BEA implies its integration with the GIG.

Defense Intelligence Mission Area (DIMA)

Consistent with the Department of Defense (DoD) Directive 8115.01, "Information Technology Portfolio Management," dated October 10, 2005, the Under Secretary of Defense for Intelligence (USD(I)) is responsible for management of the DoD portion of the Defense Intelligence Mission Area (DIMA). The USD(I) is the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. In this capacity, the USD(I) exercises the Secretary of Defense's authority, direction, and control over the Defense Agencies and DoD Field Activities that are Defense intelligence, counterintelligence, or security Components and exercises planning, policy, and strategic oversight over all DoD intelligence, counterintelligence, and security policy, plans, and programs.

USD(I) serves as the primary representative of the Secretary of Defense to the Office of the Director of National Intelligence (ODNI) and other members of the Intelligence Community (IC). The USD(I) leads DIMA and DIMA supports the DoD warfighter's strategic and operational intelligence mission needs. DIMA is adjunct to the other DoD Mission Areas and includes linkages and dependencies with the entire IC. DIMA leads DoD participation across the Defense Intelligence components, including coordinating Defense Intelligence portfolio management (PfM) with other DoD Mission Areas and coordination for DoD with the larger IC. DIMA includes all IT investments in the Military Intelligence Program (MIP) and the DoD component of the National Intelligence Program (NIP) expended by the Combat Support Agencies and the Services to satisfy intelligence mission requirements. DIMA and Associate Director of National Intelligence and Chief Information Officer (ADNI/CIO) are working toward transparent integration of each organization's capabilities in support of warfighter requirements. This integration will also incorporate coalition and allies as well as facilitation of information sharing with State and Local agencies per the Intelligence Reform and Terrorism Prevention Act of 2004.

Beginning with the FY 2008 IT Budget, the DoD is collecting the Military Intelligence Program (MIP) information technology investments for Communication and Computing Infrastructure (CCI), Information Assurance Activities (IAA), and Related Technical Activities (RTA) and include those investments within the DoD IT Budget Request. Future IT Budget Requests will be expanded to include all MIP resources, including Business and Warfighting Functional Area Applications (FAA).

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

The vision of DIMA is to integrate management of IT investments and capabilities across all intelligence functions and disciplines to preclude unnecessary duplication of capabilities by providing a balanced, integrated view of priority requirements for the near-term and the future. DIMA will leverage the USD(I) Intelligence, Surveillance and Reconnaissance (ISR) Roadmap and Strategy to align various ISR programs to identify the major opportunities for convergence, major disconnects and significant transformational and/or program acceleration opportunities that will ultimately make intelligence a warfighting operational capability responsive to the commander's needs.

The Defense Intelligence Agency (DIA) is the Executive Secretariat and Program Management Office (PMO) for DIMA and co-chair of the DIMA WG. The DIMA Working Group (WG) has identified the following functional capability domains, which are pending approval by the DIMA Stakeholders.

Analysis & Production – The integration, evaluation, and interpretation of information from a single or multiple sources into actionable intelligence for known or anticipated military, related national security, and IC consumer requirements.

Exploitation – Investments that process collected (raw) data into information appropriate for analysis

Collection – The acquisition of data from multiple collection investments (e.g. IMINT, SIGINT, MASINT, COMINT, HUMINT to include Open Source, etc.), and the provisioning of these data to exploitation elements in appropriate formats. Supporting communications are included in this domain.

Dissemination – The presentation of data, information, or intelligence in accordance with the DoD Net-Centric Strategy. (General activities to include multimedia, paper products etc.)

Enterprise IT – Investments in common core services to support one or more Intelligence lines of businesses (domains), to include:

- *Connectivity* – Includes the installation and maintenance of network pipes and wires worldwide. Also included are bandwidth and network projects (includes wireless), local area network and wide area networks regardless of data type and transport protocols. Data Handling/End user functionality – Includes data repositories, data search and manipulation, visibility, accessibility, reliability, collaborative services, and tools for producing and disseminating finished products. Includes the data layer and middleware used to access and/or manipulate data.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

- *Enterprise Architecture & Planning* - Includes IT investments supporting strategic management of IT operations.
- *Enterprise IT Systems* – Includes investments supporting the operations and maintenance of common user systems, communications, and computing infrastructure
- *Information Assurance* – Includes the technical and managerial measures designed to ensure the confidentiality possession or control, integrity, authenticity, availability, and utility of information and information systems. This definition is consistent with OMB guidance and Clinger-Cohen Act.
- *Information Policy* – Includes the processes, people and technology used to make decision about investment mix and policy, matching investments to objectives, assets allocation and balancing risk versus performance.
- *Information Security* – Includes the protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- *Management & Support* – Includes the management and operations of data centers, network operations centers, and systems operations and maintenance of continuity of operations/disaster recovery centers. Also includes system administration and monitoring, help desk operations, access control functions, close support. *Platforms* – Includes computing infrastructure and applications hosting. Facilities, hardware, and software used to provide end users with applications and tools for business support, but not to include the actual tools and data layer
- *System Maintenance* – Includes support for all activities associated with the maintenance of systems and applications

DIMA IT Investments which comprise all of the disciplined processes and systems used to implement successfully the Net-Centric Data Strategy (NCDS), i.e.: plan for, acquire, access, manage, protect, and use information management “best practice” techniques to rapidly tag, discover, horizontally integrate display, and exploit classified, open source and unclassified data.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Enterprise Management (Aligns with BMA) – Investments that enable achievement of Intelligence mission outcomes, in the areas of:

- accounting and finance
- acquisition
- human capital management
- installation and environment
- logistics
- strategic planning and budgeting
- project, program, and portfolio management
- training

Mission Management -- DIMA IT Investments which support collection requirements planning and management, operations planning and tasking (assign intelligence requirements to intelligence asset).

The goal of the selected DIMA domain investments reflected above are to provide technical solutions, which enable timely, relevant, and accurate information that is acquired, prioritized, refined and shared seamlessly across the entire IC.

Major Accomplishments

- In its' role as the DIMA PMO, DIA working with DIMA stakeholders, developed a multi-year DIMA management concept and resource plan that qualified the resources needed for mission success.
- DIMA Chief Information Officer (CIO) Summit held August 10, 2006 that provided an information briefing on DIMA portfolio management and the requirement to establish a governance structure and DIMA WG
- DIMA WG established
- DIMA Domains identified
- DIMA PfM Roles and Responsibilities Memorandum signed on January 24, 2007

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

- DIMA PFM Summit held February 1, 2007 providing DIMA Governance Process, Domain Selections and National Defense University Educational Opportunities to the attending CIO's and WG attendees

Major Planned Activities:

- Investment Binning
 - Select DIMA Owners & Domains (Programs, Systems, Initiatives)
 - Start Binning
 - De-conflict/Coordinate Binning
 - Gain Binning Approval
 - DIMA Concept of Operations
 - Select Portfolio Management Tool

Major Planned Activities Continued...

- Mission Area-Wide & Domain Specific Criteria Development
 - Identify Criteria Metrics
 - Create Portfolio Objectives
 - Establish DIMA IT Domain Risk Criteria
 - Define DIMA IT Domain Metrics
 - Enter Programs into Portfolio Management Tool

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

- Investment Analysis Against Criteria
 - Investment Analysis
 - Analyze Investments
 - Analyze Risks
 - Maximize Return/Minimize Risk
 - Prioritize Investments

- IT Investment Selection
 - Select Investments
 - Identify Investment Changes
 - Develop Portfolio Transition Plan
 - Coordinate Plan
 - Approve Domain Investments

- Control IT Investments
 - Portfolio Review/Incorporation
 - Investment Decisions
 - Documentation Coordination
 - Transition Plan
 - Recommendations

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

- Evaluate IT Investment Performance
 - Monitor & Evaluate Investments Against Domain Objectives, Metrics, Criteria & Control Recommendations
 - Reengage with Components on Disconnects
 - Adjudicate Issues
 - Update Portfolio Baseline
 - Governance Approval
 - Update DIMA Portfolio Management Tool

Enterprise Information Environment (EIEMA)

The goal of EIEMA portfolio management is to enable and support net-centric operations for warfighter, intelligence and business users by providing a common, assured, ubiquitous communications, computing and service enterprise information environment (EIE). EIEMA accomplishes this by providing a framework for identifying and meeting EIEMA user requirements, and establishing processes for working with the other Mission Areas.

The GIG assets included in the EIEMA portfolio provide EIE capabilities required to support net-centric operations. The EIE is composed of GIG assets that: 1) operate as, or that ensure, local area networks; campus area networks, tactical, operational, and strategic networks; metropolitan area networks; and wide area networks; 2) operate as, or that ensure, end-user devices, work stations, and servers that provide local, organizational, regional, or global computing capabilities; 3) include computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise capabilities; and 4) include a common set of enterprise services, called Core Enterprise Services (CES), which provide awareness of, access to, and delivery of information on the GIG.

The EIE provides the key capabilities for DoD Components to achieve assured information sharing within DoD and with partners outside DoD (e.g. intelligence community; DHS; other Federal, state and local governments; coalition partners) through implementation of the DoD Net-Centric Data Strategy (Department of Defense Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense*, December 2, 2004.)

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

EIEMA is the focal point for resolving issues by recommending solutions and alternatives for the Department's portfolio of EIE-related investments. The EIE investments are synchronized and coordinated through four EIEMA Domains: Communications (Comms), Information Assurance (IA), Core Enterprise Services (CES), and Computing Infrastructure (CI).

As directed by DoD policy, the Department of Defense Chief Information Officer (DoD CIO), as the EIEMA Lead, is charged with establishing and executing a portfolio management process for the associated portfolio of investments. Pursuant to this responsibility, the DoD CIO has determined that an Investment Review Board (IRB) and process will be used as the primary management framework for the EIEMA portfolio and associated Domain sub-portfolios.

The EIEMA IRB strives to ensure efficient and effective delivery of capabilities to the Department and to maximize return on investment to the enterprise through informed, rigorous business cases and balanced IT investment decisions across organizations and programs. EIEMA IRB and its stakeholder community will:

- Expedite the capability to advance network-centric operations by collectively assessing net-centric transformation and synchronizing capability delivery across the Department's infrastructure
- Minimize programmatic, technical, and operational risks by choosing the best mix of investments within the EIEMA portfolio
- Leverage opportunities to collaborate with other mission areas to advance mission effectiveness, identify and manage interdependencies, and foster net-centricity
- Expedite convergence toward net-centric capabilities; reduce unnecessary capability duplication; and improve efficiency, cost-effectiveness, awareness, and access to capabilities and services across the enterprise
- Transition from program-by-program investment management to end-to-end capability-based portfolio management that ensures that EIEMA portfolio recommendations inform decisions made in the Defense Acquisition System, the Joint Capabilities Integration and Development System, and the Program, Planning, Budgeting and Execution system.

Major Accomplishments: In 2006, the DoD CIO established a governance structure and process to manage the transformation of investments in the EIEMA portfolio. Key tasks included establishing a capabilities-driven portfolio management process strongly tied to DAS, JCIDS, and PPBE; fostering of a strong network of people and information across the community; and impacting decisions that drive the portfolio toward net-centricity.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

The DoD CIO established and chaired the EIEMA IRB to provide senior review of EIEMA investment recommendations. The EIEMA IRB, including all four Mission Areas and the Component CIOs, strengthened the portfolio of EIEMA investments by reprioritizing programs to fund a group of high impact, low risk computer network defense capabilities including: NIPRnet intrusion prevention; SIPRnet network access controls; host-based security systems; content filtering at INTERNET gateways; and expanded deployment of Demilitarized Zones (DMZs) to regulate access from non-DoD networks.

Major Planned Activities:

- Work with Components to identify an initial set of critical mission area capabilities and the information needed to inform the investment decision process
- Present EIEMA portfolio recommendations to the EIEMA IRB that drive the portfolio toward net-centricity
- Continue collaborating with EIEMA stakeholders to ensure the DoD CIO is maximizing delivery of EIE capabilities
- Establish methods to measure transformation over time.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

eGovernment

The Department of Defense has and continues to benefit from participation in the President's Management Agenda E-Government Initiatives and Lines of Businesses. The following are specific benefits for the Initiatives that are funded in FY 2007 and 2008:

Benefits for FY 2007

- Integrated Acquisition Environment (IAE) focused on replacing traditionally paper-based processes, such as gathering contract representation and certification or obtaining wage determination information.
- E-Rulemaking, replaced a previous legacy system with an electronic web-based notice and comment system that allows citizens and organizations to search and comment electronically on rulemaking information
- Human Resources Line-of-Business (LoB) is creating a framework for Government -wide modern, cost effective standardized and interoperable HR solutions that provide common core functionality to support the strategic management of Human Capital.
- Grant applicants have benefited from Grants.gov FIND, a central location for grant opportunities. Grants LoB has benefited DoD and the University Community by the use of a standard grant application form that brings greater consistency to the data that the components require of applicants and allows for greater oversight of the grants program.
- Federal Health Architecture LoB is a collaborative environment for Federal agencies to identify common Federal health business requirements and processes and recommend health data standards for industry to use in building health IT products.
- Business Gateway is the official resource to help business quickly find compliance information, forms and contacts from multiple Government Websites.
- E-Authentication is working to provide authentication validation services for multiple forms of identify credentials to all Federal electronic systems.

Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007

Benefits expected in FY 2008

- IT Infrastructure LoB (IOI), funded for the first time in 2007 will identify opportunities for IT infrastructure consolidation and optimization and develop government-wide solutions. It will define common performance measures for service level costs, identify best practices and develop transition plans.
- Budget Formulation and Execution LoB will build toward a budget of the future by employing standards and technologies for electronic information exchange to link budgets, execution, performance and financial information throughout all phases of annual budget cycle.
- FM LoB will provide a financial management solution that improves business performance and ensures integrity in accountability, financial controls and mission effectiveness.
- Geospatial LoB will recommend a set of common Government-wide solutions that serve the Nation's interest through more effective and efficient development, provisioning and interoperability of geospatial data and services.
- Information Systems Security was proposed as a new Line of Business to provide leadership and direction for improving effectiveness and consistency of information systems security across the Federal Government.

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

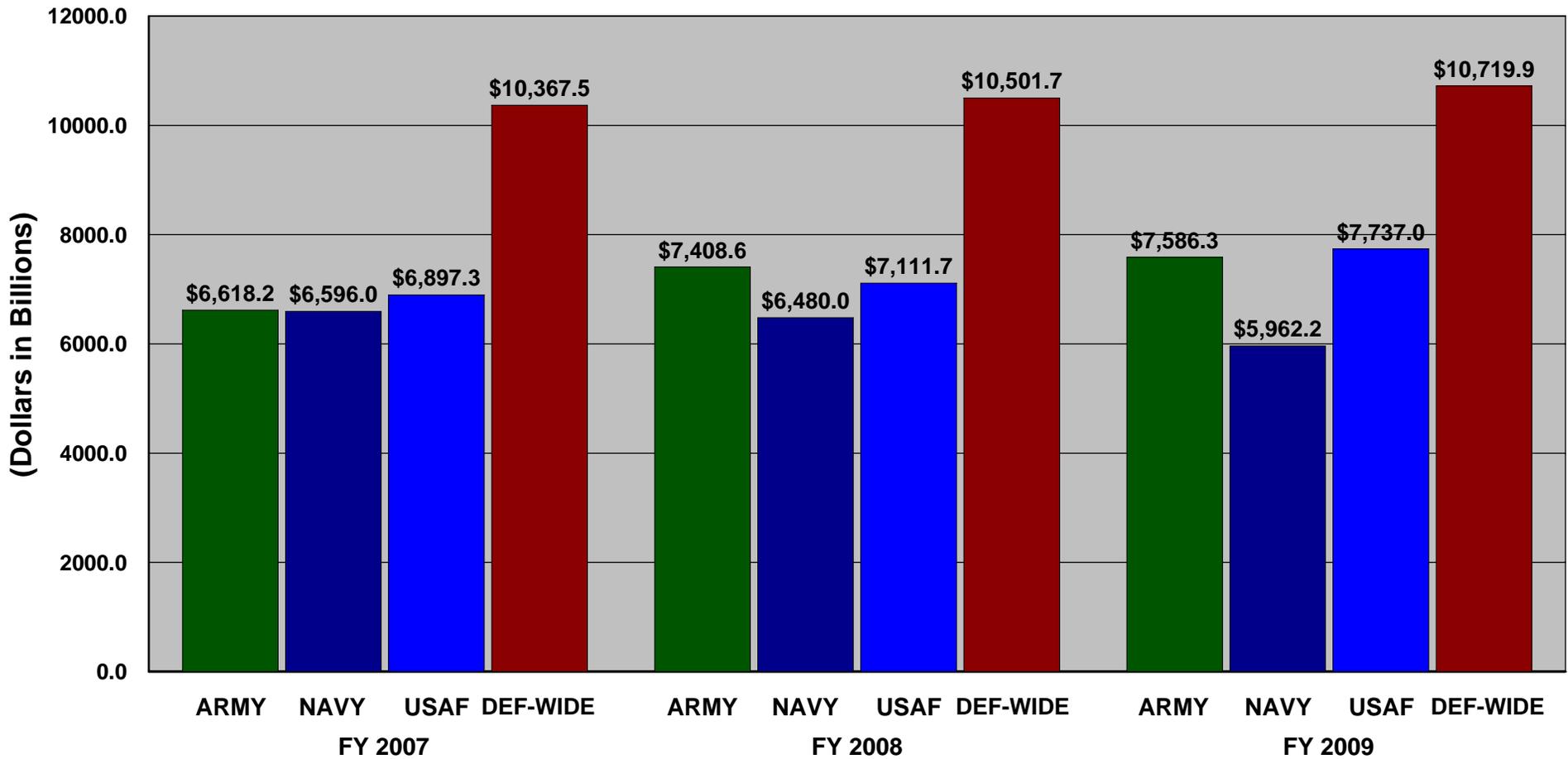
Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer

In 2003, with the approval of Congress, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) was disestablished. The Intelligence functions were transferred to the Undersecretary of Defense (Intelligence). To support the priority that the Department places on information technology transformation, the same legislation established the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)). The ASD(NII) is assigned as the Department of Defense Chief Information Officer (CIO).

The ASD(NII)/DoD CIO serves as the principle staff assistant and advisor on networks and net-centric policy, enterprise-wide integration of all information and related activities as well as information services across the Department. As the DoD Chief Information Officer, the ASD(NII)/DoD CIO provides the necessary leadership to meet the Net-Centric vision and ultimately deliver the critical enabling capabilities required by the National Defense Strategy. Transforming to a Net-Centric Force requires fundamental changes in process, policy and culture across the Department. The technology change will be significant, but the cultural shift may be even more challenging. Timely and dependable information will be available across the enterprise: from higher level headquarters and command centers, to a soldier in the city tracking insurgents, or a civilian in need of a new supplier. Ultimately, Net-Centricity means **Connecting People with Information**.

The FY2008/2009 Department of Defense IT Budget materials are available on the web at:
<https://snap.pae.osd.mil/snapit/BudgetDocs.aspx>

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**



**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2008/2009 President's Budget Request
February 2007**

COMPONENT SUMMARY

	FY2006	FY2007	FY2008	FY2009
GRAND TOTAL	\$ 34,056.44	\$ 30,478.99	\$ 31,502.06	\$ 32,005.39
DEPARTMENTS	\$ 23,683.65	\$ 20,111.45	\$ 21,000.32	\$ 21,285.51
ARMY	9,971.55	6,618.16	7,408.61	7,586.31
NAVY	6,360.01	6,595.97	6,479.97	5,962.24
AIR FORCE	7,352.09	6,897.32	7,111.73	7,736.97
DEFENSE AGENCIES	\$ 8,434.37	\$ 8,612.60	\$ 8,687.42	\$ 8,793.22
DCAA	24.27	27.99	25.92	25.78
DLA	870.80	727.76	712.34	701.55
BTA	0.00	186.71	170.54	131.46
DeCA	147.88	145.07	115.61	132.97
DFAS	403.81	415.72	384.66	365.53
DTRA	104.11	107.43	94.89	105.63
SOCOM	178.30	124.95	239.83	213.52
DISA	4,296.08	4,648.71	4,683.80	4,892.91
PFPA	7.72	8.99	9.29	8.97
DARPA	16.84	18.25	18.80	19.37
JCS	59.10	61.00	55.37	54.10
DSCA	0.00	0.00	2.51	2.00
OSD	506.77	374.27	374.57	388.66
OUSD(I)	284.90	168.93	197.96	165.12
DPMO	3.04	2.82	2.89	2.89
MDA	167.48	209.96	176.79	182.59
TRANSCOM	373.92	396.73	409.78	411.72
NSA	805.63	818.34	835.08	841.01
DSS	36.12	61.93	70.71	46.16
DCMA	147.58	107.03	106.10	101.28
FIELD ACTIVITIES	\$ 1,938.42	\$ 1,754.94	\$ 1,814.32	\$ 1,926.66
WHS	105.97	97.00	95.18	106.62
NDU	28.74	29.27	34.85	24.48
IG	14.51	16.41	15.29	16.12
DTIC	49.26	51.73	51.80	52.70
AFIS	15.18	14.65	14.87	15.10
DODDE	99.02	91.14	93.31	95.38
TMA	1,479.64	1,317.69	1,392.74	1,452.71
DHRA	146.12	137.06	116.29	163.56