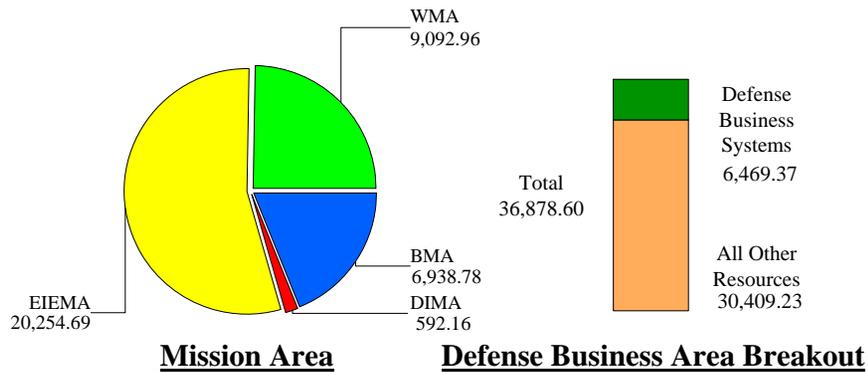


**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**



FY10/11PB Comparison (\$M)

	<u>FY2010</u>	<u>FY2011</u>	<u>Delta</u>
PB FY2010:	\$ 33,366.34	\$ 34,254.57	\$ 888.24
PB FY2011:	\$ 35,683.81	\$ 36,878.60	\$ 1,194.79
Delta:	\$ 2,317.48	\$ 2,624.03	\$ 306.55

Explain:

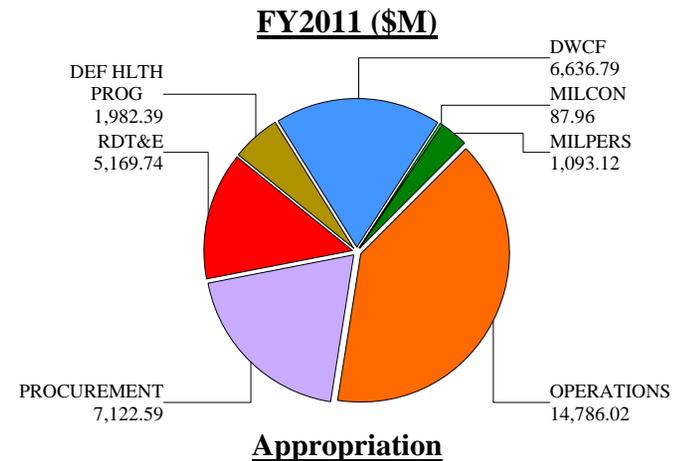
The deltas reflected between the Department of Defense FY2010 IT Budget Submission and its FY2011 IT Budget Submission at the top-line level for FY2010 and FY2011 is 6.5% and 7.1% respectively. Details about Service, DoD Agency, and DoD Activity changes can be found throughout this submission.

FY10 to FY11 Comparison (\$M)

	<u>FY2010</u>	<u>FY2011</u>	<u>Delta</u>
PB FY2011:	\$ 35,683.81	\$ 36,878.60	\$ 1,194.79

Explain:

The growth reflected in the Department of Defense IT Budget between FY2010 and FY2011 at the top-line level, just over 3%. Details about Service, DoD Agency, and DoD Activity changes can be found throughout this submission.



**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

**DoD INFORMATION TECHNOLOGY BUDGET REQUEST
BY MISSION AREA
(DOLLARS IN MILLIONS)**

MISSION AREA	FY2009	FY2010	FY2011
BUSINESS (BMA)	\$ 6,238.71	\$ 6,384.37	\$ 6,938.78
ENTERPRISE INFORMATION ENVIRONMENT (EIEMA)	\$19,752.82	\$19,594.76	\$20,254.69
DEFENSE INTELLIGENCE (DIMA)	\$ 1,298.22	\$ 631.69	\$ 592.16
WARFIGHTING (WMA)	\$10,052.83	\$ 9,072.99	\$ 9,092.96
DOD TOTALS	\$ 37,342.58	\$ 35,683.81	\$ 36,878.60

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

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

DEPARTMENT	FY2009	FY2010	FY2011
DEPARTMENT OF ARMY	\$ 9,380.33	\$ 8,010.19	\$ 8,674.70
DEPARTMENT OF NAVY	\$ 7,338.07	\$ 7,417.74	\$ 7,759.22
DEPARTMENT OF AIR FORCE	\$ 7,418.39	\$ 7,042.24	\$ 7,343.65
DEFENSE WIDE ACTIVITIES	\$13,205.79	\$13,213.65	\$13,101.04
DOD TOTALS	\$ 37,342.58	\$ 35,683.81	\$ 36,878.60

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

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

The ASD(NII)/DoD CIO serves as the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and net-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. 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 the DoD Information Enterprise 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 tracking insurgents, or a civilian in need of a new supplier. Ultimately, the role of the ASD(NII)/DoD CIO is to lead the Department to achieve an information advantage for our people and our mission partners.

Department Of Defense Information Technology Budget Overview

“Intelligence and information sharing have always been a vital component of national security. Reliable information and analysis, quickly available, is an enduring challenge... The goal is to break down barriers and transform industrial-era organizational structures into an information and knowledge-based enterprise. These concepts... will require investments in people as much as in technology to realize the full potential of these initiatives.” National Defense Strategy, June 2008

The DoD’s IT budget is designed to deliver the DoD Information Enterprise envisioned by the National Defense Strategy, the National Military Strategy, the Quadrennial Defense Review (QDR), and the Department’s GIG 2.0 CONOPS and Implementation Plan. The National Defense Strategy of June 2008 noted that providing reliable information requires not only technological changes, but also changes that break down cultural barriers impeding progress. The ASD(NII)/DoD CIO’s vision is that: *We are about mission success.* The mission accompanying this vision is based on the understanding that: *Information is one of our nation’s greatest sources of power. Our first and greatest goal, therefore, is to bring that power to the achievement of mission success in all operations of the Department: warfighting, business, and intelligence.*

The DoD Information Enterprise enables a new, net-centric way of working—constructed from the information itself, as well as a set of standards, services and procedures that enable information to be widely available to authorized users. The delivered set of services and tools will provide information and capabilities that enable end-user communities to more effectively and efficiently support mission operations. Finally, the DoD Information Enterprise includes the networks over which information travels and the security protocols that protect it.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

The DoD Information Enterprise Strategic Plan establishes goals and associated objectives that form the basis for a roadmap to guide the transformation of DoD from a stove-piped information approach to achieving the Department's net-centric information sharing vision. The Information Enterprise Strategic Plan fosters alignment of the Department's net-centric information sharing efforts, particularly those specified in the GIG 2.0 Implementation Plan, by identifying, relating and measuring the development and implementation of specific net-centric information sharing policies, programs, and initiatives. The Information Enterprise Strategic Plan also highlights how organizations are leveraging net-centric information sharing capabilities to improve the effectiveness and efficiency of processes across the Department.

Delivering this vision means:

- Treating information as a strategic asset;
- Establishing a robust, reliable, rapidly scalable and interoperable infrastructure;
- Achieving synchronized and responsive cyber space operations;
- Protecting and defending information and information systems against adverse events;
- Optimizing IT investments and more rapidly deploying IT capabilities;
- Improving and leveraging a highly skilled, innovative workforce to meet these emerging and expanding mission requirements.

The success of DoD's information sharing environment is predicated upon achieving secure information sharing within the context of a highly contested information environment. To maximize the potential of the information sharing enterprise, solutions must enable both sharing information widely and stringent protection mechanisms.

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

**Leading the Department to Achieve an Information Advantage
for our People and our Mission Partners**

<p style="text-align: center;">Information as a Strategic Asset</p> <p>A robust information environment provides DoD and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.</p> <hr style="border: 1px solid blue;"/> <p>Major enabling objectives:</p> <ul style="list-style-type: none"> • Increase Information Availability • Broaden Enterprise Services • Build Community-based Solutions • Leverage Pilots and Experimentation • Strengthen Information Sharing with Mission Partners 	<p style="text-align: center;">Interoperable Infrastructure</p> <p>A more robust, reliable, rapidly scalable and interoperable infrastructure provides connectivity and computing capabilities that allow all DoD users and mission partners to access, share, and act on the information needed to accomplish their missions.</p> <hr style="border: 1px solid blue;"/> <p>Major enabling objectives:</p> <ul style="list-style-type: none"> • Shared Computing Resources • Dynamic NetOps • Increase Transmission Capability • Enhanced Communications Interfaces • Protect DoD Internet Equities 	<p style="text-align: center;">Synchronized and Responsive Ops</p> <p>The DoD Information Enterprise (IE) infrastructure, critical assets, and capabilities are operated, secured, and defended in a synchronized manner by all DoD components to support commanders in achieving mission success.</p> <hr style="border: 1px solid blue;"/> <p>Major enabling objectives:</p> <ul style="list-style-type: none"> • Manage NetOps Risk • IE Situational Awareness and Management • Aligned NetOps Policies and Standards 	<p style="text-align: center;">Identity and Information Assurance</p> <p>A unified and resilient DoD Information Enterprise where missions continue under any cyber condition; cyber components of defense platforms perform as expected; cyber assets act effectively in their own defense; and only authorized users (including mission partners) have ready access to their information</p> <hr style="border: 1px solid blue;"/> <p>Major enabling objectives:</p> <ul style="list-style-type: none"> • IIA Community Unity • Secured Information Access • Cyber Attack Prevention • Operate Through Cyber Attacks
<p>Optimizing IT Investments</p> <p>An integrated information enterprise IT investment and IT portfolio management capability that maximizes the contribution of IT-IA investments to national security and Defense outcomes.</p>			
<p>Agile IM/IT/IA Workforce</p> <p>An agile IM/IT/IA workforce able to dynamically operate, defend, and advance the Defense Information Enterprise..</p>			

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Information as a Strategic Asset

Information is an asset: a source of power and a force multiplier. DoD and mission partners will obtain an information advantage when timely, secure and trusted information is available to all decision makers. We are moving rapidly to achieve a Service-Oriented Information Enterprise where all data assets, services and information sharing solutions must be visible, accessible, understandable and trusted by all authorized users, except where limited by law, policy or security classifications. Independent data efforts across Combatant Commands, Military Departments (MILDEPS), Defense Agencies and Field Activities, and with mission partners will be aligned and leveraged to improve data quality, integration, transparency and sharing. Once achieved, warfighters will get the critical information they need to make timely decisions affecting operations.

Interoperable Infrastructure

Achieving mission success in today's operational environment, which increasingly involves joint, combined, and non-military partners, requires a dynamic and interoperable infrastructure consisting of communications, transport, and computing capabilities. Gaining and maintaining a persistent and dominant information advantage requires robust world-wide connectivity to enable highly effective information sharing across DoD and with its external mission partners. A reliable and rapidly scalable information infrastructure is the foundation for realizing enterprise alignment through greater integration of applications, services and systems, thereby strengthening operational effectiveness and efficiency. This effort focuses on delivering the integrated information enterprise infrastructure that DoD needs to harness the power of information.

Synchronized and Responsive Operations

Synchronized and Responsive Operations will enable all DoD components to operate, secure, and defend the Information Enterprise consistently. Operating in this coordinated manner will contribute significantly to mission success, help achieve and maintain cyberspace superiority within a contested environment, and support authorized users' access to timely and trusted information when and where it is needed. This effort entails establishing GIG situational awareness from the core to the tactical edge, improving NetOps capabilities, enhancing C2 capabilities for allocating and managing IE resources, and strengthening enforcement of IE policies and standards. Information sharing across organizational boundaries and functional disciplines will be the norm. DoD personnel will increasingly rely upon timely access to trusted, secure information on a shared basis to facilitate decision-making processes at all levels of the command structure.

Identity and Information Assurance

Identity and Information Assurance focuses on assurance as a means to prepare the Information Enterprise to identify and respond to adverse events in cyber time; to ensure the integrity and authenticity of identity information (while maintaining privacy); and to protect and defend information and information systems. To achieve these objectives, it is crucial that we recognize our dependence on the Internet, that we grasp the implications of our increased reliance on external infrastructures, and that we establish protection and risk management strategies to complete our mission. Specifically, this effort will:

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

- Ensure the extended Cyber Assurance community is organized for unity of purpose and speed of action, so that each DoD organization and community of practice understands its role and works together to align policies and leverage joint decision processes.
- Enable secure mission-driven access to information and services, rendering DoD information securely accessible to all who need it and unavailable to our adversaries.
- Anticipate and prevent successful attacks on data and networks so attacks can be stopped at the perimeter and attackers quickly identified.
- Prepare for and operate through cyber degradation or attack by ensuring readiness levels are sustained and enterprise capabilities recover quickly from any incident.

Optimized IT Investments

Optimizing IT investment is based on realizing the vision to institutionalize IT management best practices. Investment review boards that govern DoD IT investments across missions are central to this vision. These review boards are tasked to review the strategic relevance of all significant investments. Optimizing IT investments will be driven by wider adoption of IT investment governance, greater utilization of enterprise architecture, increased agility in acquisition processes, coordinated management of IT portfolios, improved oversight of compliance with applicable regulations, and the establishment of an environmentally responsible IT culture focused both on cost efficiencies and the reduction of the IT influenced carbon footprint.

Agile IM/IT/IA Workforce

Timely, trusted and shared defense information is powered by transformative technology solutions that are envisioned, implemented and secured by a highly skilled workforce providing Information Management (IM), Information Technology (IT) and Information Assurance (IA) mission capabilities. Rapid technology advancements, coupled with increasing cyberspace challenges, require agile, forward thinking information resource managers and technologists who can quickly implement cost effective innovations while also enabling secured information sharing and collaboration. Strategic workforce planning supports the development of a broader balanced force with the experience, aptitude and creativity to deliver enterprise services to support the business mission, Combatant Commanders, and the warfighter.

Achieving the Department's net-centric information sharing vision depends upon improvements in the underlying capabilities of the Global Information Grid.

The Global Information Grid (GIG):

The GIG is defined as: The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Operational experiences in Iraq and Afghanistan support the continued need for the GIG 2.0 effort to eliminate barriers to information sharing that currently exist on DoD's multiple networks. A concerted effort to unify the networks into a single information environment providing timely information to commanders will improve command and control, thus increasing our speed of action. Providing an information technology (IT) / National Security Systems (NSS) infrastructure that is accessible anywhere and anytime is key to ensuring the agility of the Department and allowing our most valuable resources, our people, nearly instant access to the information they need to make decisions in the execution of their missions. In turn, the GIG must be designed and optimized to support warfighting functions of advantaged and disadvantaged users, to include mission partners, across the full range of military and National Security operations in any operational environment. The GIG must also be resilient and able to support the missions despite attacks by sophisticated adversaries.

GIG 2.0 is founded upon the following 5 characteristics:

- Global Authentication, Access Control, and Directory Services
- Information and Services "From the Edge"
- Joint Infrastructure
- Common Policies and Standards
- Unity of Command

GIG 2.0 delivers results that are timely, relevant, and focused on the needs of the warfighter while providing tools (e.g., operational outcomes, validated requirements, and architectures) to ensure stakeholder communities move toward a common and unified end state. GIG 2.0 transforms the current GIG of stove-piped systems, processes, governance, and control to a unified net-centric environment. This allows GIG 2.0 to support all DoD missions and functions in war and peace, along with supporting DoD's involvement with interagency, coalition, state, local, and non-governmental organizations (NGOs). GIG 2.0 integrates all DoD IT/NSS resources together to support the United States national interests and national strategies.

Information System Acquisition Rules

The FY2010 National Defense Authorization Act provided several authorities which will assist the Department's management of our acquisition of information systems. First, Section 804 requires the Department to develop and implement a new acquisition process for information systems based on the March 2009 recommendations of the Defense Science Board. We are developing the process and plans for its implementation, as well as drafting the required report which will update Congress on our progress.

Section 817 allows the Secretary to designate a program that meets both the definitions of a Major Automated Information System (MAIS) and a Major Defense Acquisition Program (MDAP) for treatment as only a MAIS or only an MDAP. Policy memoranda implementing this authority will be published, designating nine of the Department's largest information

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

system programs (that follow the general rule of not requiring the development of customized hardware) for treatment as MAIS only. This will provide efficient management and oversight of these and future large information system acquisitions.

MAIS Program Reporting

At the Department's request, Congress modified the Chapter 144A MAIS program reporting regime by stopping a clock that times a 5-year development period with the acquisition community's Full Deployment Decision instead of the user community's declaration of an Initial Operational Capability. This should make it easier to demonstrate compliance with Congress' desire to field rapidly executed increments of capability.

DoD Business Systems Modernization GAO Report #310675

In accordance with the "DoD IT Defense Business System (DBS) Investment Review Process Guidance", January 2009, and as mandated by the DoD CIO in the DoD CIO Memorandum, "DoD IT Portfolio Repository (DITPR)", March 17, 2005, Combatant Commands, Services, and Agencies (C/S/A) are required to register and maintain current information about all of their IT business systems in DITPR. This includes, but is not limited to, basic Business Enterprise Architecture (BEA) profile data, including OAs (both current and future/planned), Business Rules, System Functions, and Processes which must be entered and maintained in each DBS' DITPR entry. DITPR has not been approved by BTA for the assertion of compliance with the BEA. The "DoD Business Enterprise Architecture: Compliance Guidance, BEA 6.0", May 14, 2009, BEA compliance shall be asserted using one of the following methods or tools:

- The Manual Process for BEA compliance using BEA HTML (Appendix B of "DoD BEA: Compliance Guidance, BEA 6.0")
- Architecture Compliance and Requirements Traceability (ACART)
- A Component or Agency approved software tool containing the BEA

The BEA functionality in DITPR is owned by the BTA; DoD CIO has started to implement the DoD Information Enterprise Architecture, which will give guidance about assertions of compliance to all architectures and related programs in the DoD IT Portfolio. The BEA compliance assertion within the DITPR system will greatly benefit from this additional oversight.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Portfolio Management

DoD manages IT investments in IT portfolios as part of the holistic management of broader organizational and functional portfolios to support the Department's mission success; ensure efficient and effective delivery of capabilities; and maximize return on investment to the Enterprise. Each portfolio is managed using the DoD Enterprise Architecture, plans, risk management techniques, capability goals and objectives, and performance measures. The process is improving the consistency and effectiveness of decision-making processes of the Department, including the Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System (DAS), Business Capability Lifecycle (BCL), Planning, Programming, Budgeting and Execution (PPBE), Capability Portfolio Management (CPM), and Joint Concept Development and Experimentation (JCD&E), in a manner that enables better-informed decisions.

A four Mission Area construct (Warfighting, Business, Intelligence, and Enterprise Information Environment) was introduced in 2005 as an IT portfolio management and enterprise architecture construct in DoDD 8115.01 (IT Portfolio Management). These designations were purposefully very broad to provide some base level of alignment and accountability for managing the Department's IT portfolio. As the value of portfolio management became more widely recognized, DoD moved toward the management of all investments—not just IT—in portfolios. The FY 2005 Quadrennial Defense Review initiated the Capability Portfolio Management (CPM) process with pilots in four areas. In 2008, DoD issued a Capability Portfolio Management Directive (DoDD 7045.01) to expand these pilots, specifying a structure whereby all DoD programs shall be managed in a suite of portfolios. While, the exact definitions of the overall portfolios are still evolving, the idea that all DoD investments will be managed as portfolios is established.

The DoD CIO is aligning IT Portfolio Management (PfM) as part of the Department's overall processes – not as a separate, discrete process. In today's world it is difficult to separate core processes from the information flows that support them. Thus, IT PfM is a portion of the overall PfM responsibilities of process owners and organizations across the Department. Consequently, within DoD it is the responsibility of the core process owners and Components to develop architectural content to support their respective areas. The DoD CIO is realigning IT PfM and EA policy with this position. DoD CIO involvement is focused on: 1) providing frameworks and tools to support DoD EA development and use to support IT PfM; and 2) participating in portfolio management activities across DoD.

Within the CPM construct described above, Segment Architectures as defined by OMB are equivalent in the DoD EA to Capability Architectures -- sets of descriptions focused on portraying the context and rules required to achieve a desired effect through a combination of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Capability architectures enable the Department to inform and guide IT investments, identify potential gaps and overlaps and understand the broader operational constructs and segment interrelationships. The Business Enterprise Architecture (BEA) today is a good example of a capability architecture that spans multiple segments including Financial Management, Human Resources Management, Acquisition, and others. While the DoD EA spans both the DoD Enterprise level and the Component level, the segment architectures exist primarily at the DoD Enterprise level – thereby providing consistent guidance that applies to all programs, initiatives and capabilities within the Department of Defense. Component architectures extend the enterprise-level guidance, providing additional component-specific information that applies to all solutions within their organization.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

In accordance with OMB guidance, DoD is reporting its' IT/NSS budget in terms of a set of Enterprise Architecture (EA) segments—including Core Mission, Business and IT Enterprise Services segments which align with DoD's evolving portfolio management.

IT investment prioritization within and among DoD EA segments is a collaborative top-down, bottom-up process involving the DoD CIO, Joint Staff, OSD Principal Staff Assistants and the DoD Components (including Military Departments, Combatant Commands (e.g., CENTCOM), and Defense Agencies). From the top, prioritization starts with a review of the strategic objectives of the Department designed to support the National Security Strategy. The flow down is from the National Security Strategy, to the National Defense Strategy, the National Military Strategy and the Quadrennial Defense Review. Based on this guidance the Department has developed a management framework that includes guidance on developing the force and a related set of operational concepts that outline how we will prepare our military forces to achieve these strategic objectives.

The prioritization for IT investments is accomplished through collaboration and focuses on DoD warfighting functions as the key mission of the Department. Even the IT prioritization for business and IT enterprise services are focused primarily on providing support to the warfighter. IT plays a major role in each of these functions and services and the DoD CIO has a role in the decision process, as well as serving as the lead for the IT infrastructure functional area.

Each segment aligns with one primary functional area, with its own specific set of processes, structures and tools for managing its associated investments. Priority resolution that crosses functional areas is generally accomplished at the lowest level possible.

Core Mission Segments (Warfighting). The Joint Staff together with the OSD staff guides the Department's IT investments that directly support DoD's "front edge" warfighting (and other core mission) requirements. The Joint Staff has developed and implemented the JCIDS process as its primary means of prioritizing and managing the capabilities being developed, including IT and NSS. The Joint Capabilities Integration & Development System (JCIDS) process is driven by the strategic direction described above, input from the Combatant Commanders (COCOMs) in the form of Integrated Priority Lists (IPLs) and the Joint Requirements Oversight Council (JROC) by way of Joint Requirements Oversight Council Memorandums (JROCMs) and Functional Control Boards (FCBs). In addition, many of these core mission segments have tailored enterprise-level processes, structures and tools for managing their IT investments. For example, recommendations addressing the Command and Control and Battlespace Networks segment investments are supported by in-depth analyses and architectures/transition plans as well as senior level participation in the Command and Control Capability Integration Board (C2CIB).

For IT portfolio management purposes, the Department is implementing an annual Warfighting Mission Area (WMA) Assessment (or Roadmap). The initial WMA Roadmap (2008) included 27 IT investments (systems, programs, and initiatives) as a proof of concept. The 2009 WMA Assessment included 216 IT investments and, with the exception of the WMA-NC portfolio, focused on JROC interest in IT investments. The 2010 WMA Assessment will analyze and evaluate approximately 900 IT joint integration and joint information and selected independent IT investments as determined by the JCIDS gatekeeper according to CJCSI 3170.01G. The purpose of the 2010 WMA Assessment is to evaluate IT portfolios against warfighter capability requirements to impact the upcoming fiscal year budget process by recommending reductions to capability redundancies as trade space to fund warfighter mission gaps. Results of the 2010 WMA Assessment may be used to influence budget issue paper development, Chairman of the Joint Chiefs of Staff (CJCS) inputs to the Guidance for Development of the Force and Guidance for Employment of the Force, and the Chairman's Program Assessment and Chairman's Program Recommendation inputs.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Business Service Segments. The DoD Deputy Chief Management Officer (DCMO), and the business PSAs (Acquisition, Technology, and Logistics; Comptroller; and Personnel and Readiness) together with the Business Transformation Agency (BTA) guide the Department's business service segments. The governance structure and process for prioritization and management of business-related architecture and IT investments is overseen by the Investment Review Boards (IRBs) and the Defense Business System Management Committee (DBSMC) specified in Title 10 Section 2222 and 2223. The DoD guides major business system investments with the Business Capability Lifecycle, or BCL. The BCL is an important new development because until now fielding large-scale business systems was governed by the same process used to acquire complex weapon systems. The BCL is uniquely tailored to acquiring large-scale business systems within DoD that leverage Commercial Off-the-Shelf software. As such, the BCL accelerates capability delivery with less risk. 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.

The BTA utilizes an Investment Review Board¹ and Defense Business Systems Management Committee² (IRB/DBSMC) governance structure, which is led by the Deputy Secretary of Defense. The IRB/DBSMC is a single integrated decision-making structure for review and oversight of defense business capabilities and systems. The IRB/DBSMC structure ensures that all business system activities within OSD and Components adequately support the mission.

The Department has identified a core set of six Business Enterprise Priorities, or BEPs, to address DoD business transformation strategic objectives. Within BEPs, those areas that will bring the most dramatic and immediate capability improvements to the DoD's core business missions are identified. Each BEP also takes into account the critical warfighter and business requirements that cut across multiple functional areas to achieve optimal results. The Financial Visibility BEP is driving the cross-functional capabilities needed to satisfy federal mandates and to make reliable financial information accessible. The remaining five BEPs are Acquisition Visibility, Materiel Visibility, Common Supplier Engagement, Personnel Visibility, and Real Property Accountability.

The BEPs' prioritized requirements and their associated process and information changes are embodied in the Business Enterprise Architecture (BEA). As such, the BEA guides the evolution of DoD business capabilities enterprise-wide and explains what DoD must do to achieve interoperable business processes. The BEA provides context and relevance to the BEPs by embodying applicable laws, regulations, policies, standards, and frameworks imposed by internal and external sources. The BEA is not complete without describing how we will transition to the target business capabilities, which is addressed by the accompanying Enterprise Transition Plan, or ETP. The ETP is the roadmap that identifies major business transformation programs and initiatives and provides integrated schedules, metrics, and resources that guide incremental releases of target solutions to improve business capabilities.

¹ Directive Type Memorandum (08-20), "Investment Review Board (IRB) Roles and Responsibilities" <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-020.pdf>

² DESECDEF Memo "Department of Defense Business Transformation", Feb 7 2005, <http://www.dtic.mil/whs/directives/corres/pdf/dsd050207transform.pdf>

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Among the users of the BEA and ETP are the business Investment Review Boards; the Department's CIOs who manage IT portfolios; Component PEOs; program managers; and functional specialists. The BEA and ETP are transforming how DoD-level investments in business systems are managed. Now, integrated IRBs representing the core business missions of DoD hold frequent and informed discussions about business priorities and proposed IT solutions based on a common set of principles, rules, and constraints that have been mutually established and documented in the BEA. The BTA employs these three tools— the IRBs/DBSM, BEA, and ETP— to consistently guide transformation which is aligned to strategic business priorities.

DoD's five business segments: Financial Management, Acquisition, Human Resource Management, Logistics/Supply Chain Management and Installation Support align with the BEA, ETP and the IRBs.

Core Mission Segments (Intelligence). The Undersecretary of Defense for Intelligence (USD(I)) together with the Director of National Intelligence (DNI) formulates guidance for intelligence support to the Warfighter. The Intelligence Community's Information Integration Program Advisory Council (I2PAC) serves as the primary governance body for architecture and has decomposed the Intelligence Mission Area into four pillars for managing their enterprise. The primary tools used are the Intelligence Roadmap and Transition Strategy and work is proceeding on development of enterprise and segment architectures.

IT investments are a key enabler in the transformation of Defense Intelligence into an enterprise that supports the integration and synchronization of capabilities across all phases of the Intelligence, Surveillance, and Reconnaissance (ISR) mission. These capabilities include ISR planning and direction, collection, processing and exploitation, analysis and production, and dissemination for the DoD intelligence, counterintelligence and security communities. The resultant Defense Intelligence Enterprise (DIE) will enable access to the totality of intelligence resources and more effectively meet the needs of national and defense customers.

Enterprise Services Segments. The office of the DoD CIO is the primary organization responsible for IT Management and IT Infrastructure for the Department. The DoD CIO Executive Board is the principal DoD forum to advise the DoD CIO on this portion of DoD's IT portfolio. Under the DoD CIO Executive Board the Enterprise Guidance Board (EGB) serves as the senior forum in the Department responsible for guiding and developing enterprise-wide IT solution architectures, policies, and standards; including IT portfolio management. The ASD(NII)/DoD CIO has established specific processes, policies and standards for managing IT investments associated with the Cyber Identity and Information Assurance segment

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

eGovernment

The Department of Defense has and continues to benefit from the implementation of IT Management requirements supporting the President's agenda for transparency, information sharing, alignment of architectures, advancement of new technologies, and Federal-wide initiatives. The following initiatives are funded by DoD in FY2011. (Funding identified in actual dollars)

Initiative	FY10	FY11
E-Rulemaking	\$253,000	\$0
Business Gateway	\$75,000	\$0
Grants.gov	\$520,000	\$0
Financial Management LoB	\$143,000	\$0
Human Resources Management LoB	\$261,000	\$0
Grants Management LoB	\$60,000	\$0
Federal Health Architecture LoB	\$1,936,000	\$0
Information Systems Security LoB	\$1,000,000	\$300,000
Budget Formulation and Execution LoB	\$95,000	\$95,000
IT Infrastructure LoB	\$480,000	\$1,500,000
Geospatial LoB	\$44,000	\$0
E-Government Projects/Initiatives	\$14,389,000	\$13,339,000
DoD Total	\$19,256,000	\$15,234,000

Benefits:

- E-Rulemaking is a Federal-wide electronic system to promote public access to the regulatory process. Allows citizens and organizations to search and comment electronically on rulemaking information. The docket system allows the Federal departments to manage and organize materials and public comments associated with rulemakings for greater internal efficiency.
- Business Gateway is the official resource to help businesses quickly find compliance information, forms and contacts from multiple government websites.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

- The Grants.gov initiative has deployed Find and Apply functionality for Federal grants interactions. The Grants.gov Storefront provides electronic functionality for applicants and grantees, and reduces the paper-based processes that currently challenge the Federal grants environment. The initiative is designed to reduce existing inefficiencies, meet E-Gov goals, and provide benefits to both citizens and the government. Specifically, the initiative enables the government to meet many of the streamlining activities required by Public Law (PL) 106-107, Federal Financial Assistance Management Improvement Act, and other initiatives, such as deploying a unified search/find capability for grant opportunities, standard data sets, and a common mechanism and processes for applying for Federal grant funds. The Grants.gov initiative assists applicants and grantees in their efforts to streamline processes and reduce the burden associated with searching for Federal grant opportunities and completing disparate applications of Federal agencies and/or grant programs.

- FM LoB will provide a financial management solution that improves business performance and ensures integrity in accountability, financial controls and mission effectiveness. Its goals are to enhance cost savings in for future FM systems, provide standardization of business processes, promote seamless data exchange among Agencies and strengthen internal controls in financial and subsidiary systems.

- The vision of the Human Resource LOB is to create a framework for Government-wide, modern, cost effective, standardized, and interoperable HR solution(s) that provide common core functionality to support the strategic management of human capital. Driven from a business perspective rather than a technology focus, the solutions will address distinct business improvements that enhance government's performance of HR services in support of agency missions delivering services to citizens. The common solution developed by the HR LOB Federal Task Force takes a phased approach to delivering HR services through Shared Service Centers (SSCs) that will be processing centers delivering a broad array of back-office services to multiple agencies. In August of 2005, DoD was selected as an SSC along with 4 other Federal agencies.

- Grants Management Line of Business is a multi-agency initiative to develop a government-wide solution to support end-to-end grants management activities that promote citizen access, customer service, and agency financial and technical stewardship.

- Federal Health Architecture LoB (FHA) 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. FHA is sponsored by the DHHS; recommending standards to be considered for adoption to the Health Information Technology Standards Panel.

- Information Systems Security LoB (ISS LoB) establishes common solutions for information systems through Shared Services Centers (SSC). The ISS LoB has established DoD as an SSC to provide Federal Information System Security Awareness training products to agencies across the Federal enterprise.

- Budget Formulation and Execution LoB (BF&E LoB) is focused on building the 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.

- IT Infrastructure Optimization LoB (ITI LoB) supports government-wide efforts to improve the management of Federal IT infrastructure through internal efficiency and

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

effectiveness and the adoption of common solutions to improve services levels and increased cost efficiencies.

- Geospatial LoB recommends a set of common Government-wide solutions that serve the Nation's interest and the core mission of Federal agencies and their partners, through more effective and efficient development, provisioning and interoperability of geospatial data and services.
- E-Government Project/Initiative supports the implementation and oversight, within the Department, of Federal-wide IT initiatives such as Internet Protocol Version 6 (IPv6), Cloud Computing, Enterprise Architecture, and IM/IT/IA workforce development.

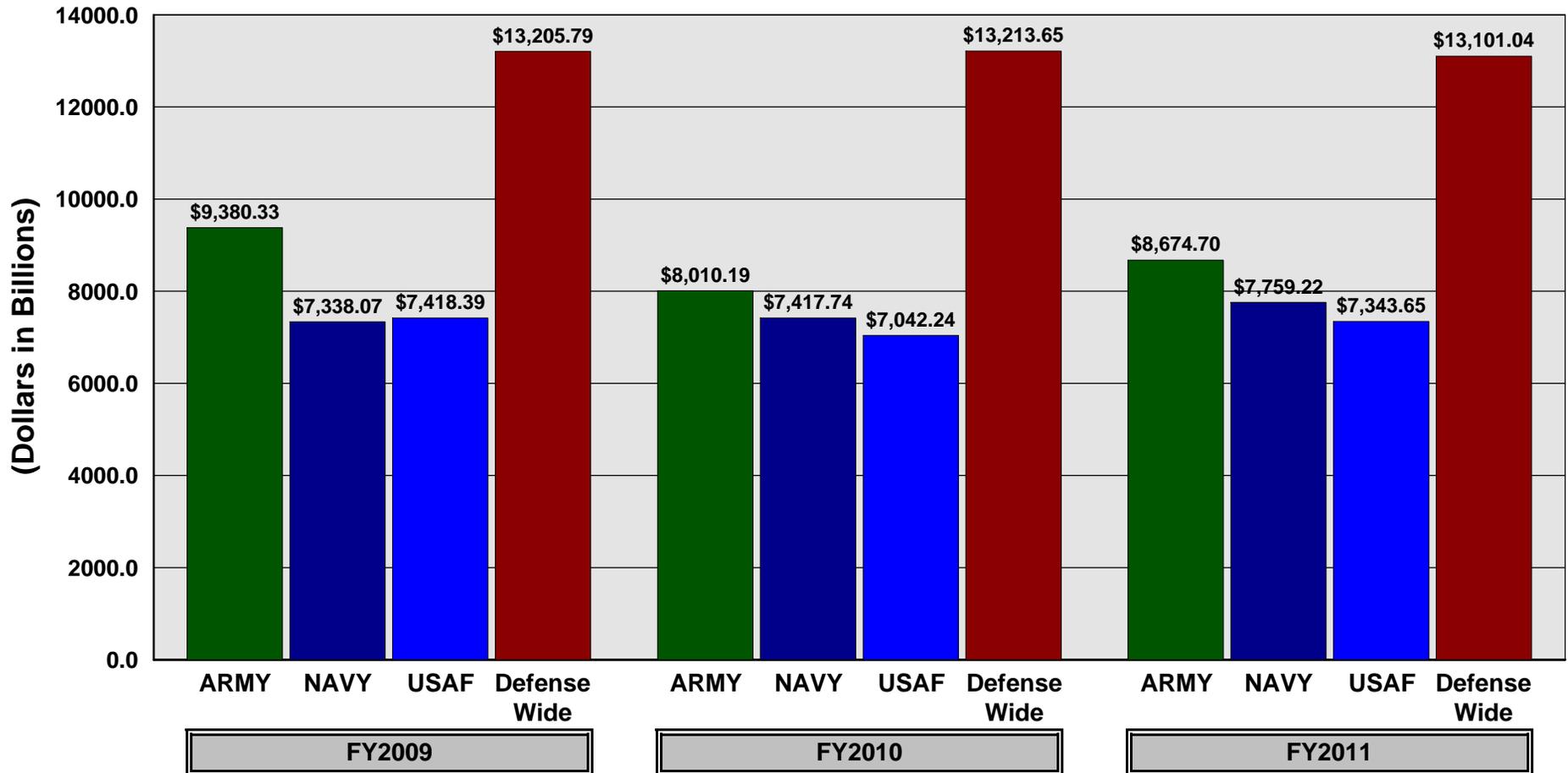
Notes:

The FY2011 Department of Defense IT Budget materials are available on the web at: <https://snap.pae.osd.mil/snapit/BudgetDocs2011.aspx>

Resources provided to the Department of Defense for Spectrum Relocation and Base Closure and Realignment are not included in the President's Budget Request for Information Technology.

Department of Defense
 Fiscal Year (FY) 2011 IT President's Budget Request
 March 2010

COMPONENT SUMMARY



**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

COMPONENT SUMMARY

	FY2009	FY2010	FY2011
GRAND TOTAL	\$ 37,342.58	\$ 35,683.81	\$ 36,878.60
DEPARTMENTS	\$ 24,136.78	\$ 22,470.16	\$ 23,777.56
AIR FORCE	7,418.39	7,042.24	7,343.65
ARMY	9,380.33	8,010.19	8,674.70
NAVY	7,338.07	7,417.74	7,759.22
DEFENSE AGENCIES	\$ 10,928.00	\$ 10,900.14	\$ 10,406.61
BTA	218.46	191.49	198.52
DARPA	79.31	83.13	44.54
DCAA	23.31	30.33	30.01
DCMA	125.61	121.40	121.05
DeCA	87.40	88.50	124.93
DFAS	448.83	426.46	431.91
DISA	4,757.14	5,191.12	5,093.87
DLA	862.35	964.39	956.11
DSCA	4.51	2.27	2.43
DSS	62.28	55.65	33.49
DTRA	95.81	101.22	115.97
DTSA	9.03	10.71	10.58
JCS	61.96	87.08	111.01
MDA	206.15	193.90	165.97
NSA	972.52	915.95	901.98
OSD	420.83	468.85	401.44
OUSD(I)	1,724.25	1,183.97	945.57
PFFA	14.85	16.15	17.03
SOCOM	381.15	313.83	281.67
TRANSCOM	371.30	453.74	409.76
USD_ATL	0.97	0.00	8.79
FIELD ACTIVITIES	\$ 2,277.80	\$ 2,313.51	\$ 2,694.42
DHRA	213.62	246.80	321.17
DMACT	14.03	13.73	12.68
DODDE	92.17	93.28	94.59
DPMO	2.69	4.53	5.09
DTIC	17.24	16.79	22.49
IG	28.57	26.12	19.66
NDU	15.17	25.43	23.68
TMA	1,746.77	1,675.24	1,982.39
WHS	147.54	211.60	212.69

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank