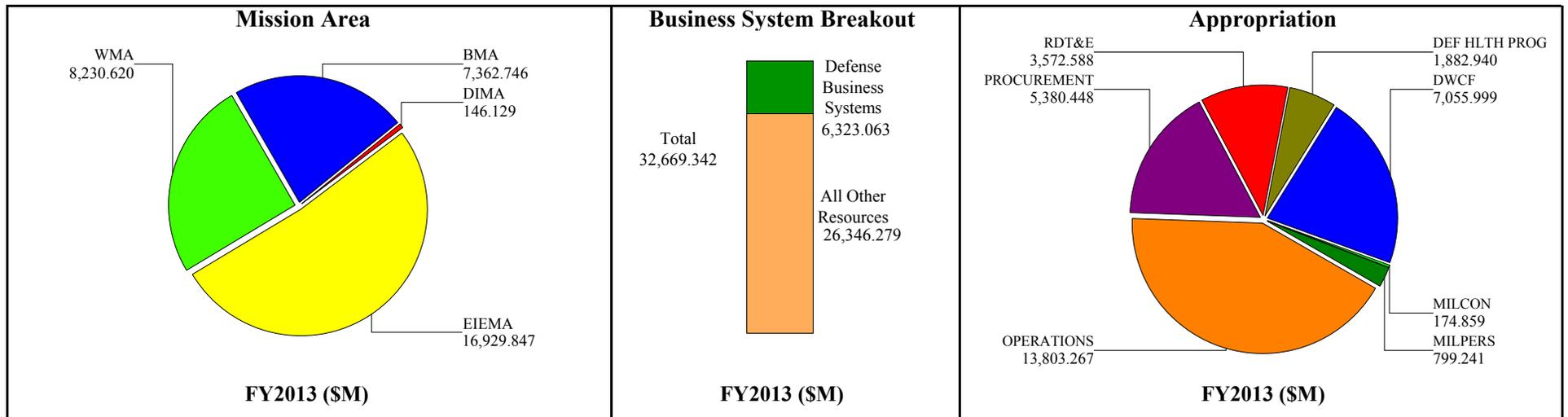


**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**



FY12 to FY13 Comparison (\$M)	FY2012	FY2013	Delta	FY12/FY13PB Comparison (\$M)	FY2012	FY2013	Delta
PB FY2013:	33,032.166	32,669.342	-362.824	PB FY2012:	38,449.180	35,831.810	-2,617.370
				PB FY2013:	33,032.166	32,669.342	-362.824
				Delta:	-5,417.014	-3,162.468	
Explanation: The vast majority of the -\$362.8M change can be directly attributable to DoD senior-leadership decisions, policy and management direction in constructing the Department's FY2013 President's Budget with decreases to the Overseas Contingency Operations (OCO) funding and Joint Tactical Radios. The Army has increases for the War-fighter Information Tactical, Increments 2 and 3 and the Navy increasing Next Generation Enterprise Network.				Explanation: The vast majority of the -\$3.2B change can be directly attributable to the removal of DoD's Cybersecurity or Identity and Information Assurance budget and other classified IT reporting to the Classified IT Budget submission. The DoD minimizes the national security risk by collecting, aggregating, and reporting cyber, identity, information assurance, and other classified information technology activities in a classified annex to the Information Technology budget submission.			

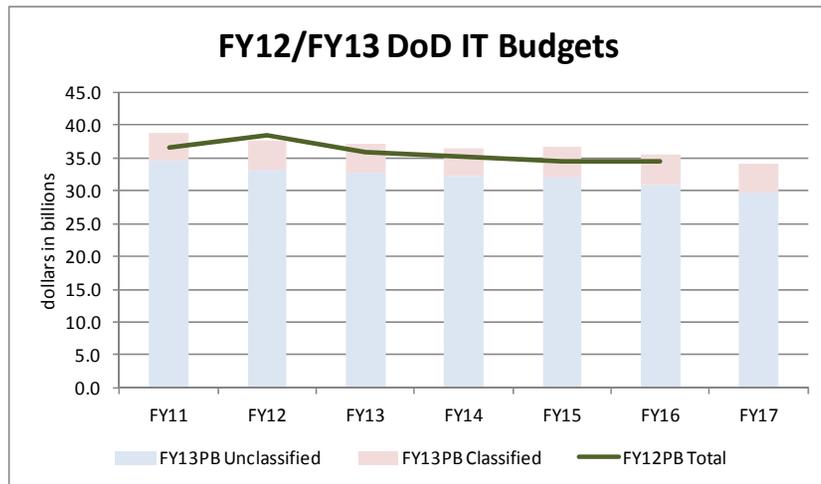
**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

Department of Defense Fiscal Year (FY) 2013 IT President's Budget Request Overview

Department of Defense (DoD) Chief Information Officer (CIO)

The Department of Defense (DoD) FY13 total Information Technology Budget Request is \$37.0B and represents a \$0.5B (1.3%) decrease from the FY12 enacted. This request includes both unclassified (\$32.7B) and classified (\$4.3B) investments.



Source: FY12 DoD IT President's Budget and FY13 DoD IT President's Budget Submission

	<i>(dollars in thousands)</i>						
	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Army							
Unclassified	10,157,282	8,867,196	8,912,804	8,782,843	9,055,033	8,696,819	8,149,428
Classified	1,112,418	808,968	885,996	787,825	842,655	808,387	946,399
Total	11,269,700	9,676,164	9,798,800	9,570,668	9,897,688	9,505,206	9,095,827
Navy							
Unclassified	7,533,492	7,119,007	7,007,920	6,540,538	6,178,697	5,897,612	5,762,970
Classified	446,405	438,835	471,825	462,167	486,296	439,425	476,581
Total	7,979,897	7,557,842	7,479,745	7,002,705	6,664,993	6,337,037	6,239,551
Air Force							
Unclassified	6,087,625	6,032,000	5,609,761	5,931,779	5,982,593	5,504,200	4,845,386
Classified	645,433	598,640	589,279	687,250	775,258	816,380	571,076
Total	6,733,058	6,630,640	6,199,040	6,619,029	6,757,851	6,320,580	5,416,462
Defense-Wide							
Unclassified	10,662,793	11,013,963	11,138,857	10,894,183	10,734,108	10,743,092	10,901,484
Classified	2,094,630	2,604,313	2,382,291	2,409,143	2,462,880	2,461,464	2,513,248
Total	12,757,423	13,618,276	13,521,148	13,303,326	13,196,988	13,204,556	13,414,732
Department of Defense							
Unclassified	34,441,192	33,032,166	32,669,342	32,149,343	31,950,431	30,841,723	29,659,268
Classified	4,298,886	4,450,756	4,329,391	4,346,385	4,567,089	4,525,656	4,507,304
Total	38,740,078	37,482,922	36,998,733	36,495,728	36,517,520	35,367,379	34,166,572

Source: FY13 DoD IT President's Budget Submission

The United States and its international partners face a world of complex national security challenges. Nowhere is this more apparent than in cyberspace. Cyberspace has emerged as a critical operational element in the military environment and ensuring the availability and dominance of cyberspace is a major challenge facing the DoD. Consequently, the DoD's networks are a mission critical resource that underpins Information Operations, Command and Control, logistics, finance, transportation, medical, maintenance and other activities.

The DoD's Cybersecurity or Identity and Information Assurance budget is a collection of efforts intended to defend and secure the information networks. The collection, aggregation, and reporting of detailed Cybersecurity and other classified IT reporting in an unclassified environment creates a risk to national security which may reveal information on US Cybersecurity strategic plans, operational capabilities, technological capabilities, or infrastructure vulnerabilities.

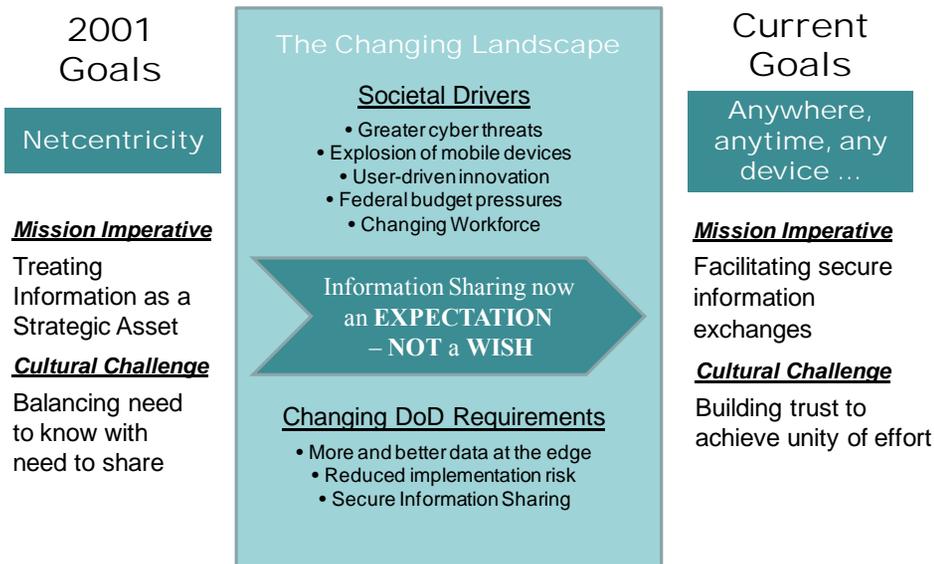
The DoD minimizes the national security risk by collecting, aggregating, and reporting cyber, identity, information assurance, and other classified information technology activities in a classified annex to the Information Technology budget submission. A copy of the FY13 classified IT annex can be obtained by contacting the office of the DoD Chief Information Officer.

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Department Of Defense Information Technology Budget Overview

The DoD CIO serves as the advisor to the Secretary of Defense and Deputy Secretary of Defense on networks; command and control (C2); communications; enterprise-wide integration of DoD information matters; information technology (IT); information management (IM); spectrum management; network operations; information systems; cybersecurity (CS); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; and related matters. As the DoD Chief Information Officer, the 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 DoD CIO is to lead the Department to achieve an information advantage for our people and our mission partners.

The Evolving DoD CIO challenge



As of January 2012, the Office of the Assistant Secretary of Defense for Networks and Information Integration was disestablished and assumed the title of DoD CIO.

“There is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communications networks and assured access to cyberspace.” Quadrennial Defense Review, February 2010

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), the Department’s Strategic Management Plan (SMP) and the Department’s Global Information Grid (GIG) 2.0 Concept of Operations (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 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.

Department of Defense Fiscal Year (FY) 2013 IT President's Budget Request Overview

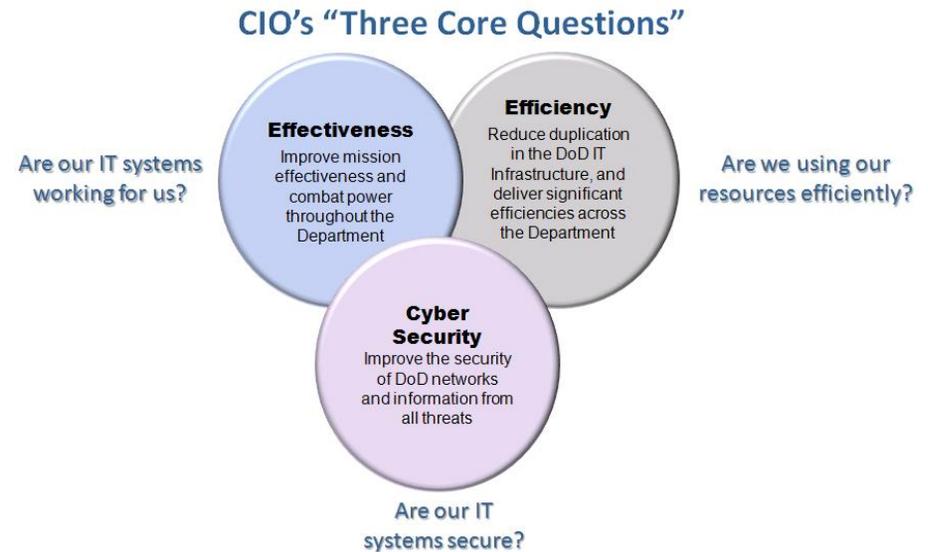
The DoD Information Enterprise (IE) enables a new, net-centric way of working—constructed from the information itself, as well as a set of standards, services and procedures as described in the DoD Information Enterprise Architecture - that enable information to be widely available to authorized users. 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.

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 information sharing vision. The Information Enterprise Strategic Plan fosters alignment of the Department's information sharing efforts, particularly those specified in the GIG 2.0 Implementation Plan, by identifying, relating and measuring the development and implementation of specific 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) 2013 IT President's Budget Request
Overview**

**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;">Cybersecurity</p> <p>DoD can accomplish its missions in the face of cyber warfare by a capable adversary.</p> <hr style="border: 1px solid blue;"/> <p>Major enabling objectives:</p> <ul style="list-style-type: none"> • Resilience to operate through cyber attacks • Agile, safe information sharing with mission partners • Robust attack detection diagnosis and response • Information security
<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) 2013 IT President's Budget Request Overview

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.

The Department continues to take important steps to become more open, transparent and accountable by providing data and information that is of importance to the public. DoD continues to provide greater access to the Department's data with 32 datasets and 270 tools posted on Data.gov. The DoD Open Government website was updated to improve usability and DoD's Freedom of Information Act (FOIA) website now includes over 300,000 pages of FOIA responses online. DoD is also using social media technologies to foster participatory dialog with the public and increase engagement through blogs, apps, mobile resources, and collaboration tools.

The Department is committed to realizing the value of cloud computing by driving delivery and adoption of a secure, dependable DoD Enterprise Cloud Computing Environment that improves IT efficiencies, enhances mission effectiveness, meets mission needs and supports anywhere, anytime, information access, in alignment with Federal and Department-wide IT efficiency initiatives. The Department has specific challenges that pose careful adoption considerations, especially in areas of cyber security. DoD plays a key role in Federal Cloud Computing initiatives such as the Federal Risk and Authorization Management Program that is addressing security concerns. Within the DoD, our early cloud initiatives, such as the Defense Information Systems Agency's (DISA) Rapid Access Computing Environment (RACE), are evolving to enable migrations of legacy applications to cloud services. This DoD Enterprise Cloud is providing the foundation for the Air Force's efforts to virtually integrate three geographically separate personnel and finance centers: the Air Force Personnel Center, Air Reserve Personnel Center, and the Air Force Financial Services Center, starting with the consolidation of their customer relationship management and knowledge management capabilities. The Air Force has already realized benefits that include avoiding \$250,000 in technical refresh and license costs. In addition, by centralizing Air Force personnel services on a single-access platform with a secure entry point serving 1.7 million customers they have experienced a quantum leap in service center productivity—1.3 million transactions and 560,000 calls with 100 percent case resolution. Cost avoidance is projected to be \$12 million during the Five Year Defense Plan by using the Enterprise cloud rather than the separate capabilities.

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.

Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview

In August 2010, the Secretary of Defense directed the consolidation of IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs and to improve the DoD's ability to execute its missions while defending its networks against growing cyber threats. In response, the Department has identified opportunities to consolidate DoD IT infrastructure through several initiatives, one of which is data center and server consolidation which is consistent with the Federal Data Center Consolidation Initiative (FDCCI). DoD Components are considering all options for achieving consolidation that includes migrating infrastructure to Defense Information Systems Agency (DISA) enterprise computing centers (DECCs), valid commercial options, cross-Component co-hosting, virtualization and cloud computing, to name a few. The current DoD goal is to reduce data centers to 428 by FY15. DoD has exceeded its target of 52 closures for FY11 with the closure of 57 data centers. DoD continues to identify additional data centers for closure and is aggressively pursuing consolidation and virtualization.

Based on our quarterly data center closure tracking, the DoD has projected the closing of 97 data centers in FY12. Based on the DoD Data Center Consolidation Plan we project closing 127 data centers in FY13. DoD is on target to directly save \$300 million and avoid an additional \$325-\$369 million in FY2013. Most of these ongoing reductions derive from costs no longer needed for the data centers closed in FY2011 and FY2012. Remaining reductions derive from costs after 127 data centers close throughout FY13.

DoD's data center inventory, used to derive the cost reduction estimates above, has significant shortcomings and missing data. The DoD is placing greater reliance on a recently developed FDCCI Task Force's Total Cost of Ownership model to help model consolidation decision making and derive cost savings data. Consequently, DoD continues to refine and validate the asset inventory information and support means to improve estimating accuracy.

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.

Defensive Cybersecurity

The DoD continues significant efforts to improve cyber security. As part of this emphasis, DoD published the Defense Strategy for Operations in Cyberspace and DoD strengthened operational control over the department's information and information systems via the creation of US Cyber Command. The department is also aggressively improving cyber information sharing models so that DoD knowledge of cyber incidents and attacks can be shared quickly with the federal government, our allies and coalition partners, and with our defense industrial partners. As the department moves to consolidate, centralize, and automate more of its information infrastructure, DoD is redesigning core cyber security policies, processes, and technologies to be more efficient and to give the department more consistent information and mission protection. The department is

Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview

consolidating the purchase of cyber security tools and capabilities in order to deploy protection and cyber attack detection and diagnosis systems that are shared across all DoD organizations. Deploying department-wide capabilities is more efficient and enhances our ability to protect information and mission. The DoD efforts to improve cybersecurity are in partnership with the rest of the federal government and others in order to provide consistent standards, easier information sharing, and mission protection across the full spectrum of DoD and Federal missions. DoD also continues to build a more capable cyber security workforce that can keep pace with the rapidly changing nature of the technology, threat, and DoD operations.

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 the DoD 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.

In 2011, DoD conducted over 10 Agency-level TechStats for major IT investments. Outcomes included improved governance, accelerated delivery of capability (Teleport Generation 3), program termination (Joint Tactical Radio System-Ground Mobile Radios (JTRS-GMR), and reduced scope (Air Force Expeditionary Combat Support System (ECSS) and Mission Planning System Increment 4 (MPS Inc 4)). MPS Inc 4 was restructured to focus on fielding enhanced capabilities on specific aircraft and achieved a life cycle cost avoidance of \$150.7 million.

Agile IT/Cybersecurity Workforce

Timely, trusted and shared defense information is stored on and shared through transformative technology solutions that are designed, secured and implemented by a highly skilled workforce providing IT, Cybersecurity, and IT acquisition mission capabilities. Rapid technology advancements, coupled with increasing cyberspace challenges, require agile, fiscally responsible, and forward thinking individuals to architect, design, develop, acquire, operate, maintain and protect DoD IT/cyber resources, as well as strategic policy makers, planners and managers who oversee the governance of the DoD Information Enterprise. Strategic workforce planning supports the development of a broader balanced workforce with the experience, aptitude and creativity to deliver enterprise services to support the business mission, Combatant Commanders, and the warfighter.

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) 2013 IT President's Budget Request
Overview

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/ National Security Systems (IT/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. GIG 2.0 integrates all DoD IT/NSS resources together to support the United States national interests and national strategies.

DoD Business Systems Modernization GAO Report #310675

The Business Enterprise Architecture (BEA) guides and constrains investments and implementation of interoperable defense business system solutions. The Strategic Management Plan (SMP) is the key driver for the BEA, defining goals and objectives. The enterprise transition plan (ETP) is the transition plan for BEA implementation. A more detailed discussion of the BEA and ETP are included in the Portfolio Management section.

The SMP establishes specific business goals that directly support the Strategic Goals of the QDR, as well as further articulates changes needed in the Department's business domain, while ensuring unity of effort across the enterprise. The latest SMP covers a two year period, fiscal years 2012-2013 and includes seven overarching business goals:

1. Strengthen and right-size the DoD total workforce
2. Strengthen DoD financial management
3. Build agile and secure information technology capabilities
4. Increase the buying power of the DoD

Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview

5. Increase operational and installation energy efficiency
6. Re-engineer/use end-to-end business processes
7. Create agile business operations that support contingency missions

Each business goal is supported by key initiatives needed to achieve the business outcome.

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 Operational Activities (OAs) (both current and future/planned), Capabilities, System Functions, and Processes which must be entered and maintained as a part of each DBS' DITPR entry. The Business Enterprise Architecture (BEA) guides and constrains investments and implementation of interoperable defense business system solutions. As such, this BEA profile data is used to further identify the compliance criteria by which DBSs must assert and be accountable for by the Investment Review Boards (IRBs). Per the "DoD Business Enterprise Architecture: Compliance Guidance, BEA 8.0", March 11, 2011, BEA compliance shall be asserted using one of the following methods or tools:

- The Manual Process for BEA compliance using BEA HTML located at: <http://www.us.army.mil/suite/doc/27406386>; or
- ACART™, the process for usage can be located at: <http://www.us.army.mil/suite/doc/27405819>.

Portfolio Management

The Department's IT investments are critical in supporting our military forces in their mission of protecting our Nation's security. These investments support the effective and efficient use of information as a strategic asset in military and business operations to improve the operational effectiveness and security of the information and networks transporting the information. DoD manages IT investments in 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 content and organizing constructs within the DoD Enterprise Architecture, plans, risk management techniques, capability goals and objectives, and performance measures. This will improve 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 (IT PfM) and Enterprise Architecture (EA) 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

Department of Defense Fiscal Year (FY) 2013 IT President's Budget Request Overview

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 capability portfolios.

The DoD CIO aligns IT investment management as part of the Department's overall processes – not as a separate, discrete process. IT PfM is a portion of the overall 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 aligning IT investment management and EA policy focusing 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. 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 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. Component architectures extend the enterprise-level guidance, providing additional component-specific information that applies to all solutions within their organization.

In accordance with OMB guidance, DoD is reporting its IT/NSS budget in terms of a set of EA segments. To align with DoD's evolving portfolio management construct, the DoD IT budget can be described through the following segments:

- Business Services
- Enterprise Services
- Core Mission (Warfighting)
- Core Mission (Intelligence)

IT investment prioritization within and among DoD EA segments is a collaborative process involving the DoD CIO, Joint Staff, OSD Principal Staff Assistants (PSA), Deputy Chief Management Officer (DCMO) 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.

Department of Defense Fiscal Year (FY) 2013 IT President's Budget Request Overview

Business Service Segments: The DoD DCMO, and the business PSAs (Acquisition, Technology, and Logistics; Comptroller; and Personnel and Readiness) 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 NDAA FY 12 recently collapsed the IRBs under the PSAs into a single IRB under the DCMO, which guides major business system investments using the Business Capability Lifecycle (BCL). BCL consolidates governance and acquisition oversight using the IRB framework. The JCIDS and the DAS governance processes and associated documentation, developed for weapon systems, are integrated into the BCL process and use a business case for executive decision making. BCL is uniquely tailored to acquiring large-scale business systems within DoD that leverage Commercial Off-the-Shelf software. Through a disciplined process of analysis and review, BCL provides the problem definition, solution analysis, program justification and acquisition oversight model that addresses known issues with delivering timely business solutions and at reduced cost and risk. By requiring capability delivery in increments of 18 months or less, a best practice used by industry in implementing IT systems, BCL minimizes the risk of delivering capabilities and will enable DoD to keep pace with advances in information technology.

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

The Department is shifting its focus from functional activities to business outcomes by taking an end-to-end view of its processes and the data that goes through them. The Department recognizes the urgent need to develop special acquisition processes to more rapidly acquire and deploy IT in order to keep pace with technology evolution. This requires new methodologies to help investment managers (IRBs and DBSMC) make better decisions about IT investments and architecture development. At the operational level, business systems will use process improvement methodologies to ensure they are implementing efficient solutions that execute processes seamlessly. At all levels, the Department is establishing performance measures and tracking performance to verify whether planned outcomes are actually realized.

The BEA is the enterprise architecture for the DoD Business Mission Area, including defense business systems. The BEA, guided by overarching Departmental business priorities detailed in the SMP, defines the business capabilities required to support those priorities and the combination of enterprise systems and initiatives that enable those capabilities. The BEA includes laws, regulations, data standards, business rules and other requirements to which systems must comply. The BEA helps guide and constrain portfolio management by requiring compliance/alignment of systems to enterprise requirements as well as providing visibility into system migration plans. The BEA also provides visibility to the business enterprise on current and target system environments and funding, insuring investment decisions support the Department's transformational efforts.

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) 2013 IT President's Budget Request Overview

The Enterprise Transition Plan (ETP) focuses specifically on those business systems that are new or being modernized and provides the Department's roadmap accordingly. It identifies the governance and strategic framework DoD uses to manage its investments, describes how those investments are part of the Department's overarching management reform efforts, outlines key improvement initiatives and provides specific information regarding each of its business system investments. The prioritized requirements of the PSAs and their associated process and information changes are embodied in the 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 business operations of the Department 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.

Among the users of the BEA and ETP are the IRB/DBSMC; the Department's CIOs who manage IT portfolios; Component Program Executive Offices; program managers; and functional specialists. The BEA and ETP are transforming how DoD-level investments in business systems are managed. Through the IRB process, the DoD PSAs hold frequent and informed discussions about business priorities and proposed IT solutions based on a common set of principles, rules, and constraints which are mutually established and documented in the BEA. The DCMO employs these three tools— the IRBs/DBSMC, BEA, and ETP— to consistently guide transformation which is aligned to strategic business priorities.

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. The DoD CIO Executive Board membership is composed of DoD Principal Staff Assistants, and CIOs of the Military Departments, Joint Staff, Intelligence Community, Joint Warfighting Community and the Office of the Secretary of Defense. Under the DoD CIO Executive Board are three Review Groups, Information Assurance Enterprise Review Group, Enterprise Services Review Group, and the Architecture & Standards Review Group which serve as senior forums in the Department. They are responsible for guiding and developing enterprise-wide IT solution architectures, policies, and standards. The DoD CIO has established specific processes, policies and standards for managing IT investments associated with the Cyber Identity and Information Assurance segment. Enterprise services investments include those supporting a robust, reliable, efficient and interoperable infrastructure.

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 JCIDS process is driven by the strategic direction described above, input from the Combatant Commanders in the form of Integrated Priority Lists and the Joint Requirements Oversight Council by way of Joint Requirements Oversight Council Memorandums and Functional Capability Boards. In addition, many of these core mission segments have tailored enterprise-level processes, structures and tools for managing their IT investments.

Core Mission Segments (Intelligence): The Undersecretary of Defense for Intelligence (USD(I)) together with the Director of National Intelligence formulates guidance for intelligence support to the Warfighter. The Intelligence Community's Information Integration Program Advisory Council serves as the primary governance body for architecture

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

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 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 will enable access to the totality of intelligence resources and more effectively meet the needs of national and defense customers.

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. E-Government Projects/Initiatives support the implementation and oversight, within the Department, of Federal-wide IT initiatives such as Enterprise Architecture, Federal Information Sharing, Cloud Computing, E-Government Analysis & IT Portfolio Management, IT Consolidation, and IM/IT/IA workforce development. The following initiatives will be funded by DoD agency contributions³ in FY 2013.

(Funding identified in actual dollars)

Initiative	FY12	FY13
Financial Management LoB	\$142,857	\$142,857
Human Resources Management LoB	\$260,870	\$260,870
Grants Management LoB	\$59,316	\$58,589
Federal Health Architecture LoB	\$2,094,000	\$2,094,000
Geospatial LoB	\$42,000	\$42,000
Budget Formulation and Execution LoB	\$105,000	\$105,000
DoD Total	\$2,704,043	\$2,703,316

³ Agency contributions reflect commitments of funding and/or in-kind services provided by partner agencies to initiative managing partner agencies in support of developing, implementing, and/or migrating to E-Government common solutions. Contribution amounts are determined annually through collaborative, inter-agency E-Government initiative governance structures and are subject to approval by OMB.

Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview

Objective of eGovernment Initiatives⁴:

- Financial Management LoB / Managing Partner, Department of the Treasury - The Financial Management Line of Business is focused on financial systems improvements in coordination with the Chief Financial Officers Council. There are thousands of interrelated systems and hundreds of stakeholders, including the Chief Financial Officer, Chief Information Officer, and Chief Administrative Officer communities across all Departments and agencies.
- Human Resources LOB / Managing Partner, Office of Personnel Management - DoD is one of the approved service providers for the Human Resources (HR) LOB. Core HR services are provided by DoD for its Military Services, Defense Agencies and civilian customer agencies through the Defense Civilian Personnel Advisory Service and the Defense Finance and Accounting Service. This initiative allows the DoD to optimize the cost of managing HR systems and processes across a worldwide customer base and to reduce costs of performing these functions individually. Involvement in the HR LOB permits the DoD to benefit from best practices and government-wide strategic HR management. Participation in the HR LOB presents opportunities to partner with other providers in obtaining core functional changes for jointly-used commercial HRIT products. This approach contributes to DoD's goal for implementation of efficient, state-of-the-art, and cost-effective enterprise HR solutions.
- Grants Management LoB / Managing Partner, National Science Foundation (NSF) - To explore the use of NSF's Research.gov portal by DoD components responsible for the award and administration of research grants and agreements.
- Federal Health Architecture LoB / Managing Partner, Department of Health and Human Services - Federal Health Architecture (FHA) coordinates government-wide solutions for interoperable and secure health information exchange that address agency business priorities, while protecting citizen privacy. In addition to the DoD, FHA serves the needs of more than twenty Federal agencies in domains as diverse as veterans' healthcare, public health monitoring, long-term care and disability services, research, and tribal health services.
- Geospatial LoB / Managing Partner, Department of the Interior - Improved access to geospatial information to improve productivity, improve mission delivery, and increased service to citizens. Geospatially enabling traditional business data to improve business process efficiency, allow for geographically based work planning and investment processes, assist in infrastructure asset tracking, improve mission delivery, and promote the use of business intelligence in the Department's decision support systems.
- Business Formulation and Execution LoB / Managing Partner, Department of Education - The Budget Formulation and Execution LoB provides significant benefits to the DoD by encouraging best practices crossing all aspects of Federal budgeting -- from budget formulation and execution to collaboration, human capital needs, and providing tools and resources.

⁴ OMB Report to Congress on the benefits of the President's E-Government Initiatives for Fiscal Year 2012.

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Notes:

The FY2013 Department of Defense IT Budget materials are available on the web at: <https://snap.pae.osd.mil/snapit/BudgetDocs2013.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.

The IT spending amount presented in the FY13 ANALYTICAL PERSPECTIVES was based on local estimates submitted by agencies in early January. In early February, after the budget had gone to print, the Department of Defense submitted its official FY13 Presidents Budget Request for IT spending. When these revisions are factored into overall Federal IT spending, the decrease from FY12 to FY13 is \$586 million, or 0.7% (vs. \$929 million, or 1.2% found in the Budget Chapter). The revised amounts were used in the presentation on February 13, 2012.

The DoD amounts presented on the Office of Management and Budget Information Technology Dashboard (ITDB) (<http://www.itdashboard.gov>) may not reflect the amounts presented in this budget document. Adjustments made to the DoD OMB Exhibit 53 Submission for the Defense Security Cooperation Agency (DSCA) and Pentagon Force Protection Agency (PFPA) in FY 2011 and the US Air Force (AF) throughout the Future Year Defense Plan (FYDP) were not reflected on the ITDB at the time of this document's publication (March 2012).

<i>(dollars in thousands)</i>	FY 2011	FY 2012	FY 2013	FY 2014
OMB ITDB*	34,887,926	33,770,441	32,846,030	32,314,755
DSCA Adjustments	+2,379			
PFPA Adjustments	+17,642			
AF Adjustments	-466,755	-738,275	-176,688	-165,412
Congressional Submission**	34,441,192	33,032,166	32,669,342	32,149,343

* DoD Exhibit 53 Submission to OMB on February 6, 2010

** DoD Unclassified FY13 President's Budget Request to Congress

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

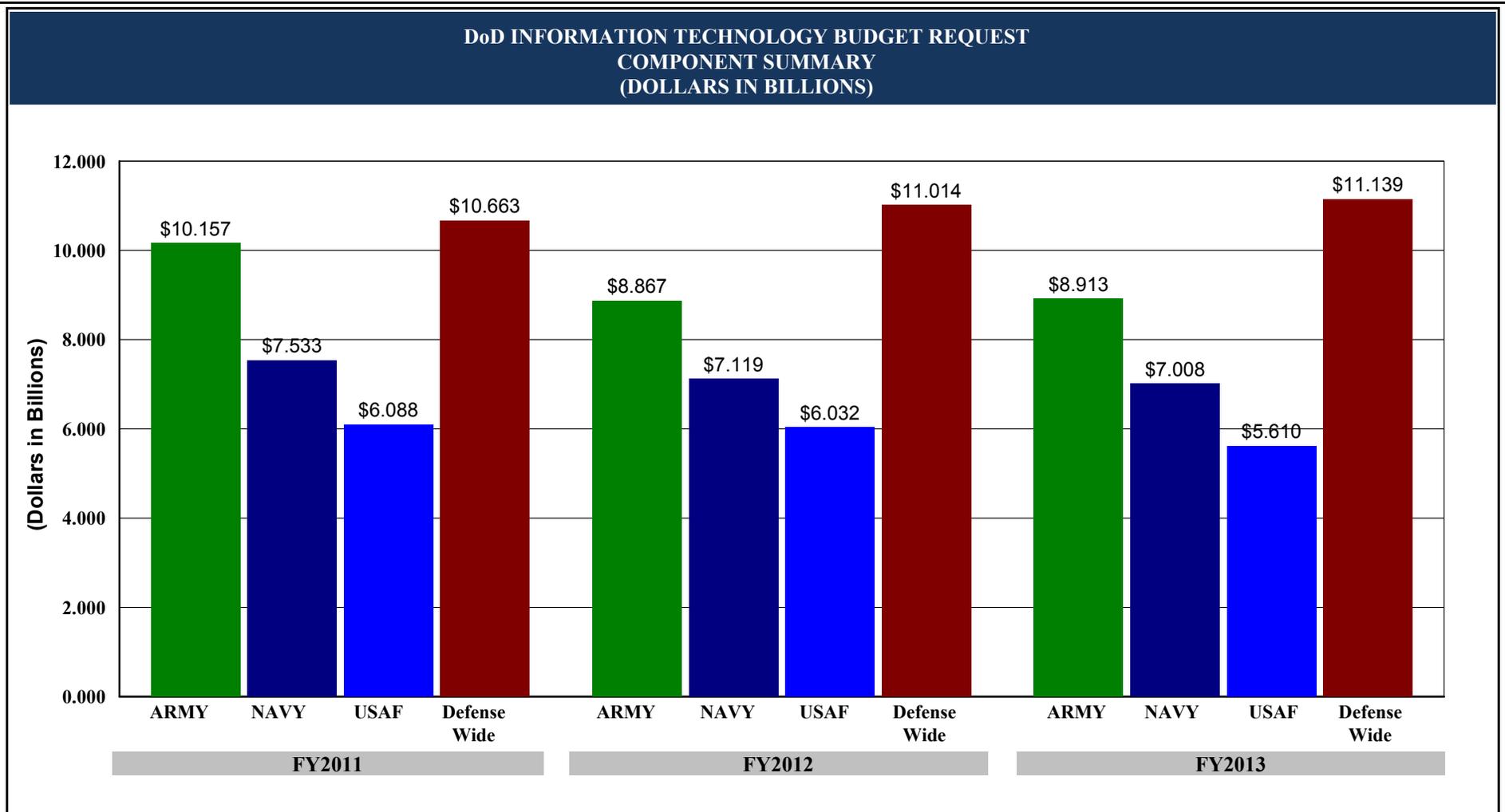
**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY DEPARTMENT (DOLLARS IN MILLIONS)			
DEPARTMENT	FY2011	FY2012	FY2013
DEPARTMENT OF ARMY	\$10,157.282	\$8,867.196	\$8,912.804
DEPARTMENT OF NAVY	\$7,533.492	\$7,119.007	\$7,007.920
DEPARTMENT OF AIR FORCE	\$6,087.625	\$6,032.000	\$5,609.761
DEFENSE WIDE ACTIVITIES	\$10,662.793	\$11,013.963	\$11,138.857
DOD TOTALS	\$34,441.192	\$33,032.166	\$32,669.342

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**



**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY COMPONENT (DOLLARS IN MILLIONS)			
	FY2011	FY2012	FY2013
GRAND TOTAL	\$34,441.192	\$33,032.166	\$32,669.342
DEPARTMENTS	\$23,778.399	\$22,018.203	\$21,530.485
AIR FORCE	\$6,087.625	\$6,032.000	\$5,609.761
ARMY	\$10,157.282	\$8,867.196	\$8,912.804
NAVY	\$7,533.492	\$7,119.007	\$7,007.920
DEFENSE AGENCIES	\$8,087.201	\$8,352.799	\$8,564.706
BTA	\$86.284	\$0.000	\$0.000
DARPA	\$31.978	\$32.937	\$33.925
DCAA	\$29.070	\$26.428	\$29.357
DCMA	\$143.735	\$113.202	\$129.492
DeCA	\$80.026	\$114.444	\$97.642
DFAS	\$417.835	\$416.592	\$412.518
DISA	\$4,784.203	\$4,918.936	\$4,999.056
DLA	\$1,067.358	\$1,109.491	\$1,227.098
DSCA	\$2.379	\$3.424	\$3.526
DSS	\$24.713	\$32.205	\$39.408
DTRA	\$128.861	\$110.752	\$114.589
DTSA	\$4.607	\$5.266	\$5.599
JCS	\$112.619	\$91.990	\$112.142
MDA	\$175.470	\$157.333	\$144.568
OSD	\$41.148	\$28.519	\$24.075
PFPA	\$17.642	\$18.036	\$16.906
SOCOM	\$472.293	\$597.518	\$567.741
TRANSCOM	\$452.099	\$516.316	\$547.431
USD(AT&L)	\$14.881	\$59.410	\$59.633
FIELD ACTIVITIES	\$2,575.592	\$2,661.164	\$2,574.151

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

BY COMPONENT - continued (DOLLARS IN MILLIONS)			
	FY2011	FY2012	FY2013
DCMO	\$0.000	\$10.599	\$9.855
DHRA	\$328.975	\$278.040	\$302.432
DMACT	\$12.951	\$9.586	\$27.607
DODDE	\$76.317	\$77.445	\$78.998
DPMO	\$5.223	\$4.900	\$4.500
DTIC	\$20.880	\$19.583	\$19.083
IG	\$32.165	\$28.878	\$25.972
NDU	\$12.727	\$12.233	\$13.885
TMA	\$1,908.132	\$2,008.254	\$1,882.940
WHS	\$178.222	\$211.646	\$208.879

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY SEGMENT (DOLLARS IN MILLIONS)				
SEGMENT	FY2011	FY2012	FY2013	
ACQUISITION	\$542.266	\$496.972	\$509.242	
BATTLESPACE AWARENESS-ENVIRONMENT	\$262.004	\$255.392	\$150.153	
BATTLESPACE AWARENESS-ISR	\$202.125	\$177.975	\$146.129	
BATTLESPACE NETWORKS	\$4,005.750	\$4,519.869	\$4,391.532	
BUILDING PARTNERSHIPS	\$4.207	\$4.289	\$5.639	
BUSINESS SERVICES TBD	\$21.982	\$33.581	\$33.199	
COMMAND & CONTROL	\$2,562.137	\$2,242.396	\$2,049.884	
CORE MISSION TBD	\$36.198	\$27.733	\$36.864	
DOD IT INFRASTRUCTURE	\$17,361.091	\$15,982.203	\$16,381.245	
ENTERPRISE SERVICES TBD	\$43.054	\$42.791	\$44.489	
FINANCIAL MANAGEMENT	\$753.967	\$745.358	\$796.091	
FORCE APPLICATION	\$1,199.171	\$875.079	\$669.900	
FORCE MANAGEMENT	\$82.067	\$46.422	\$48.870	
FORCE TRAINING	\$345.848	\$305.799	\$395.558	
HEALTH	\$951.218	\$1,154.175	\$1,038.584	
HUMAN RESOURCE MANAGEMENT	\$1,774.487	\$1,830.063	\$1,818.136	
INSTALLATION SUPPORT	\$151.992	\$198.424	\$186.967	
IT MANAGEMENT	\$585.051	\$529.847	\$504.113	
LOGISTICS/SUPPLY CHAIN MANAGEMENT	\$3,201.615	\$3,120.928	\$2,980.527	
PROTECTION	\$354.962	\$442.870	\$482.220	
DOD TOTALS	34,441.192	33,032.166	32,669.342	

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST SEGMENTS BY COMPONENT (DOLLARS IN MILLIONS)			
ACQUISITION	FY2011	FY2012	FY2013
ARMY	\$87.150	\$88.130	\$97.797
NAVY	\$192.290	\$187.287	\$192.602
AIR FORCE	\$155.004	\$89.216	\$80.583
DEFENSE WIDE	\$107.822	\$132.339	\$138.260
	\$542.266	\$ 496.972	\$ 509.242
BATTLESPACE AWARENESS-ENVIRONMENT	FY2011	FY2012	FY2013
ARMY	\$113.942	\$113.364	\$15.248
NAVY	\$78.044	\$63.622	\$59.740
AIR FORCE	\$70.018	\$78.406	\$75.165
	\$262.004	\$ 255.392	\$ 150.153
BATTLESPACE AWARENESS-ISR	FY2011	FY2012	FY2013
ARMY	\$10.095	\$7.303	\$4.375
NAVY	\$44.184	\$33.654	\$17.859
AIR FORCE	\$147.846	\$137.018	\$123.895
	\$202.125	\$ 177.975	\$ 146.129
BATTLESPACE NETWORKS	FY2011	FY2012	FY2013
ARMY	\$1,076.421	\$1,799.771	\$2,044.981
NAVY	\$875.305	\$1,154.974	\$969.925
AIR FORCE	\$1,243.500	\$695.343	\$570.914
DEFENSE WIDE	\$810.524	\$869.781	\$805.712
	\$4,005.750	\$ 4,519.869	\$ 4,391.532
BUILDING PARTNERSHIPS	FY2011	FY2012	FY2013
DEFENSE WIDE	\$4.207	\$4.289	\$5.639
	\$4.207	\$ 4.289	\$ 5.639

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
BUSINESS SERVICES TBD	FY2011	FY2012	FY2013
ARMY	\$6.810	\$9.020	\$7.624
NAVY	\$9.978	\$9.838	\$11.476
AIR FORCE	\$1.580	\$0.624	\$0.614
DEFENSE WIDE	\$3.614	\$14.099	\$13.485
	\$21.982	\$ 33.581	\$ 33.199
COMMAND & CONTROL	FY2011	FY2012	FY2013
ARMY	\$523.108	\$503.125	\$491.557
NAVY	\$732.123	\$449.422	\$434.120
AIR FORCE	\$969.341	\$899.568	\$787.331
DEFENSE WIDE	\$337.565	\$390.281	\$336.876
	\$2,562.137	\$ 2,242.396	\$ 2,049.884
CORE MISSION TBD	FY2011	FY2012	FY2013
ARMY	\$31.538	\$24.024	\$32.267
NAVY	\$2.732	\$1.498	\$1.923
AIR FORCE	\$0.097	\$0.062	\$0.083
DEFENSE WIDE	\$1.831	\$2.149	\$2.591
	\$36.198	\$ 27.733	\$ 36.864
DOD IT INFRASTRUCTURE	FY2011	FY2012	FY2013
ARMY	\$5,038.527	\$3,853.854	\$3,663.274
NAVY	\$3,928.563	\$3,521.311	\$3,779.087
AIR FORCE	\$2,079.097	\$2,353.020	\$2,384.133
DEFENSE WIDE	\$6,314.904	\$6,254.018	\$6,554.751
	\$17,361.091	\$ 15,982.203	\$ 16,381.245
ENTERPRISE SERVICES TBD	FY2011	FY2012	FY2013
NAVY	\$7.624	\$4.082	\$4.147
DEFENSE WIDE	\$35.430	\$38.709	\$40.342
	\$43.054	\$ 42.791	\$ 44.489

Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview

SEGMENTS BY COMPONENT - continued			
(DOLLARS IN MILLIONS)			
FINANCIAL MANAGEMENT	FY2011	FY2012	FY2013
ARMY	\$240.509	\$143.345	\$106.622
NAVY	\$147.949	\$135.832	\$166.212
AIR FORCE	\$97.178	\$132.313	\$168.850
DEFENSE WIDE	\$268.331	\$333.868	\$354.407
	\$753.967	\$ 745.358	\$ 796.091
FORCE APPLICATION	FY2011	FY2012	FY2013
ARMY	\$799.725	\$431.337	\$280.245
NAVY	\$172.540	\$132.988	\$155.414
AIR FORCE	\$226.906	\$310.754	\$234.241
	\$1,199.171	\$ 875.079	\$ 669.900
FORCE MANAGEMENT	FY2011	FY2012	FY2013
ARMY	\$5.329	\$4.230	\$4.230
NAVY	\$46.791	\$17.368	\$20.143
AIR FORCE	\$9.840	\$8.027	\$9.965
DEFENSE WIDE	\$20.107	\$16.797	\$14.532
	\$82.067	\$ 46.422	\$ 48.870
FORCE TRAINING	FY2011	FY2012	FY2013
ARMY	\$309.340	\$285.602	\$373.300
NAVY	\$5.363	\$5.346	\$3.998
AIR FORCE	\$11.809	\$9.527	\$10.837
DEFENSE WIDE	\$19.336	\$5.324	\$7.423
	\$345.848	\$ 305.799	\$ 395.558
HEALTH	FY2011	FY2012	FY2013
ARMY	\$5.967	\$5.489	\$6.198
NAVY	\$3.073	\$3.166	\$3.260
AIR FORCE	\$1.156	\$0.046	\$0.000
DEFENSE WIDE	\$941.022	\$1,145.474	\$1,029.126
	\$951.218	\$ 1,154.175	\$ 1,038.584

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
HUMAN RESOURCE MANAGEMENT	FY2011	FY2012	FY2013
ARMY	\$667.378	\$613.520	\$699.829
NAVY	\$384.771	\$488.990	\$395.532
AIR FORCE	\$215.278	\$257.756	\$249.276
DEFENSE WIDE	\$507.060	\$469.797	\$473.499
	\$1,774.487	\$ 1,830.063	\$ 1,818.136
INSTALLATION SUPPORT	FY2011	FY2012	FY2013
ARMY	\$77.883	\$58.248	\$59.122
NAVY	\$27.928	\$29.015	\$26.586
AIR FORCE	\$42.432	\$106.252	\$98.592
DEFENSE WIDE	\$3.749	\$4.909	\$2.667
	\$151.992	\$ 198.424	\$ 186.967
IT MANAGEMENT	FY2011	FY2012	FY2013
ARMY	\$73.592	\$63.301	\$44.093
NAVY	\$4.265	\$1.962	\$1.863
AIR FORCE	\$33.007	\$25.640	\$26.103
DEFENSE WIDE	\$474.187	\$438.944	\$432.054
	\$585.051	\$ 529.847	\$ 504.113
LOGISTICS/SUPPLY CHAIN MANAGEMENT	FY2011	FY2012	FY2013
ARMY	\$1,028.603	\$828.428	\$879.078
NAVY	\$857.319	\$861.347	\$743.757
AIR FORCE	\$558.125	\$589.429	\$484.190
DEFENSE WIDE	\$757.568	\$841.724	\$873.502
	\$3,201.615	\$ 3,120.928	\$ 2,980.527
PROTECTION	FY2011	FY2012	FY2013
ARMY	\$61.365	\$35.105	\$102.964
NAVY	\$12.650	\$17.305	\$20.276
AIR FORCE	\$225.411	\$338.999	\$304.989
DEFENSE WIDE	\$55.536	\$51.461	\$53.991
	\$354.962	\$ 442.870	\$ 482.220
DoD Totals	\$34,441.192	\$33,032.166	\$32,669.342

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Overview**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY MISSION AREA (DOLLARS IN MILLIONS)			
MISSION AREA	FY2011	FY2012	FY2013
BUSINESS	\$7,397.527	\$7,579.501	\$7,362.746
DEFENSE INTELLIGENCE	\$202.125	\$177.975	\$146.129
ENTERPRISE INFORMATION ENVIRONMENT	\$17,989.196	\$16,554.841	\$16,929.847
WARFIGHTING	\$8,852.344	\$8,719.849	\$8,230.620
DOD TOTALS	\$34,441.192	\$33,032.166	\$32,669.342