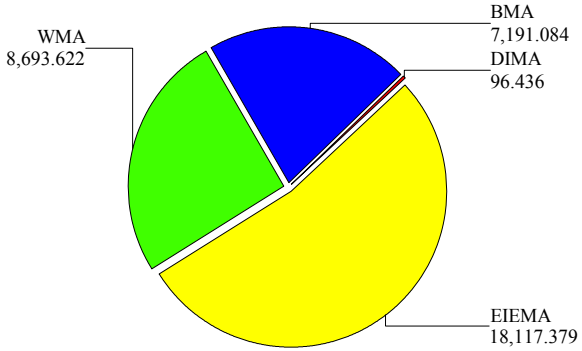
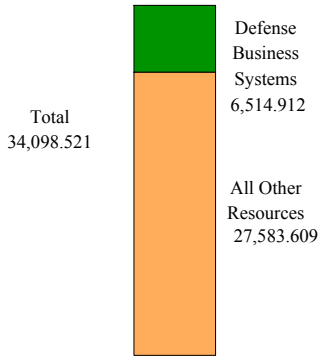
Department of Defense
Fiscal Year (FY) 2014 IT President's Budget Request
Overview

Mission Area



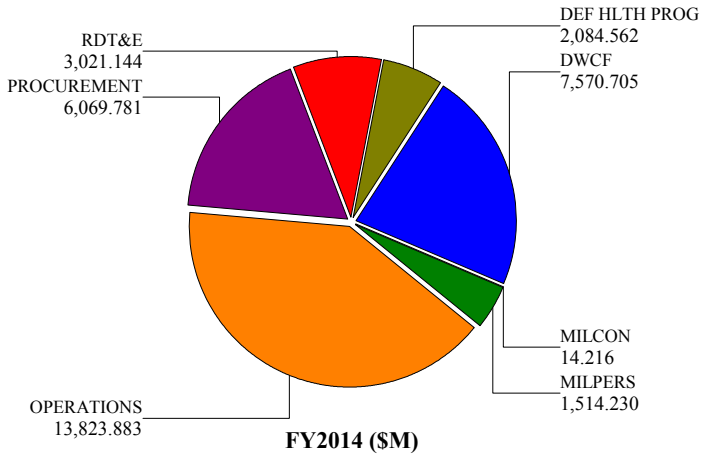
FY2014 ($M)

Business System Breakout



FY2014 ($M)

Appropriation



FY2014 ($M)

FY13 to FY14 Comparison ($M)	FY2013	FY2014	Delta
PB FY2014:	34,123.014	34,098.521	-24.493

Explanation:

Horizontal (-$24.5M, .07%)

The decrease of $24.5 million from FY 2013 represents an insignificant change in the Department of Defense's IT budget. The majority of change is due to FY 2014 DoD Component budget decisions to align IT spending with leadership direction and priorities. FY 2013 amounts are lower than expected due operations being conducted under a lengthy Continuing Resolution and sequestration. See Component Overview's for additional detail.

FY13/FY14PB Comparison ($M)	FY2013	FY2014	Delta
PB FY2013:	32,669.342	32,149.343	-519.999
PB FY2014:	34,123.014	34,098.521	-24.493
Delta:	1,453.672	1,949.178	

Explanation:

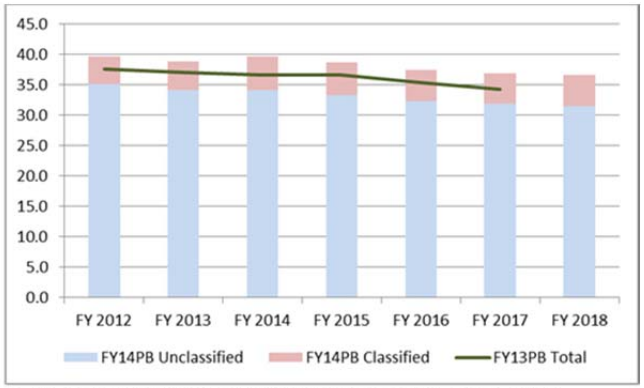
Vertical (+$1,949M, 6%)

Significant increases between the FY 2013 and FY 2014 President's Budget submissions are attributed to improving transparency by expanding IT reporting to better address Defense Business System (DBS) and their certification, IT consolidation efforts, standardization, enterprise licensing, implementation of enterprise solutions, Medical Development Technology, and military personnel costs.

Page left intentionally blank

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

The Department of Defense (DoD) FY14 total Information Technology Budget Request is $39.6B and represents a $0.8B (2.0%) increase from the FY13 enacted. This request includes both unclassified ($34.1B) and classified ($5.5B) investments. Consistent with administration guidance, the DoD IT Budget (non-cyber) remains constant in FY 2014 and projects a $2.6 billion decrease over the FY14-FY18 Future Year Defense Plan (FYDP). Cyberspace Operations has been increased approximately 18% in FY 2014 and is projected to remain relatively constant over the FYDP.



Source: FY 2013 DoD President's IT Budget and FY 2014 DoD President's IT Budget

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 Cyberspace Operations and Information Assurance budget is a collection of efforts intended to operate, defend, and secure the information networks. The collection, aggregation, and reporting of detailed Cyberspace and other classified IT reporting in an unclassified environment creates a risk to national security which may reveal information on US Cyberspace 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 FY14 classified IT annex can be obtained by contacting the office of the DoD Chief Information Officer.

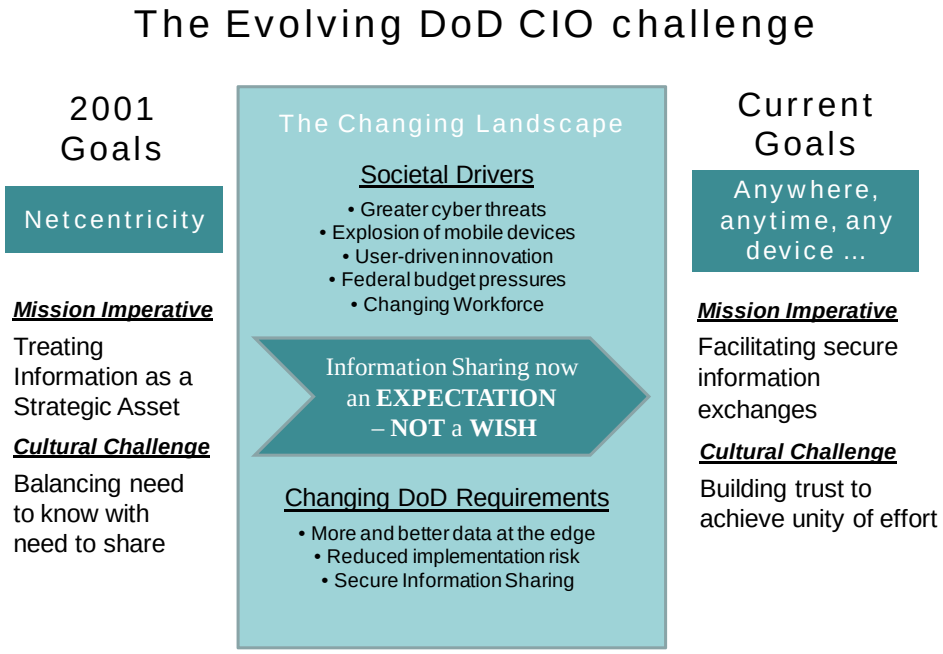
(dollars in thousands)

	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
Army							
Unclassified	10,273,039	9,811,701	9,725,381	9,395,743	9,058,051	9,010,978	8,839,289
Classified	468,012	536,218	669,364	702,889	609,897	631,920	654,032
Total	**10,741,051**	**10,347,919**	**10,394,745**	**10,098,632**	**9,667,948**	**9,642,898**	**9,493,321**
Navy							
Unclassified	7,495,064	7,613,270	7,210,651	6,770,841	6,472,287	6,436,282	6,481,746
Classified	412,878	528,218	535,394	675,446	671,207	649,255	657,282
Total	**7,907,942**	**8,141,488**	**7,746,045**	**7,446,287**	**7,143,494**	**7,085,537**	**7,139,028**
Air Force							
Unclassified	6,252,871	5,285,742	5,449,284	5,694,280	5,367,087	4,937,155	4,562,611
Classified	667,286	856,981	1,415,082	1,352,603	1,242,071	1,102,765	1,098,603
Total	**6,920,157**	**6,142,723**	**6,864,366**	**7,046,883**	**6,609,158**	**6,039,920**	**5,661,214**
Defense-Wide							
Unclassified	11,011,159	11,412,301	11,713,205	11,359,954	11,383,303	11,495,127	11,608,319
Classified	3,007,921	2,765,826	2,880,362	2,666,495	2,630,111	2,606,973	2,668,936
Total	**14,019,080**	**14,178,127**	**14,593,567**	**14,026,449**	**14,013,414**	**14,102,100**	**14,277,255**
Department of Defense							
Unclassified	35,032,133	34,123,014	34,098,521	33,220,818	32,280,728	31,879,542	31,491,965
Classified	4,556,097	4,687,243	5,500,202	5,397,433	5,153,286	4,990,913	5,078,853
Total	**39,588,230**	**38,810,257**	**39,598,723**	**38,618,251**	**37,434,014**	**36,870,455**	**36,570,818**

Source: FY 2014 DoD President's IT Budget Submission

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.



"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 cyperspace." Quadrennial Defense Review, February 2010

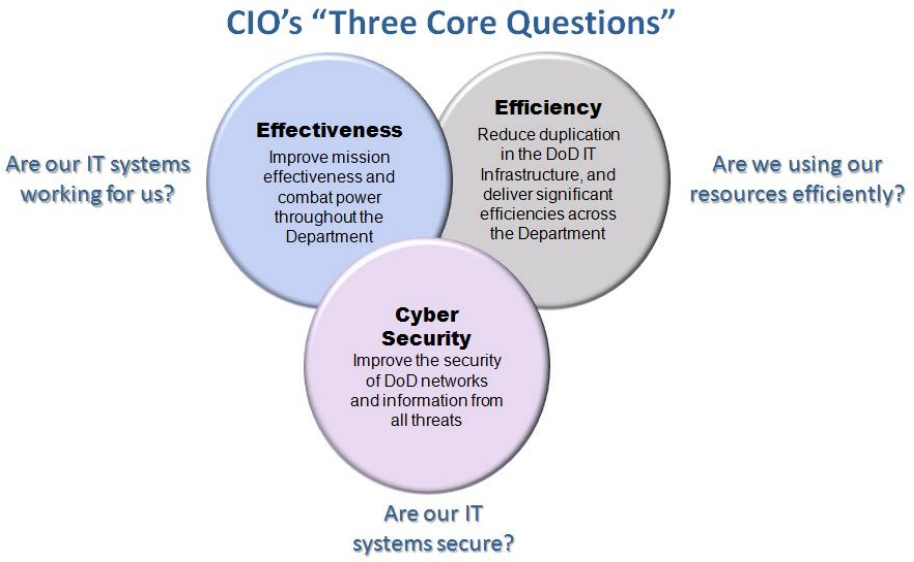
The DoD's IT budget is designed to deliver the DoD Information Enterprise envisioned by the National Defense Strategy, the National Military Strategy, the Quadrennial Defense Review (QDR), the Department's Strategic Management Plan (SMP) and the Department's Global Information Grid (GIG) 2.0 Concept 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 asset. Our first and greatest goal, therefore, is to leverage that asset (or those assets) to the achievement of mission success in all operations of the Department: warfighting, business, and intelligence.*

Department of Defense
Fiscal Year (FY) 2014 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. The IT environment investments operate in over 6,000 locations worldwide, supporting the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department. 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.

Joint Information Environment (JIE)

The DoD CIO is leading the implementation of the Joint Information Environment (JIE) initiative with a collaborative team of experts from DoD CIO, the Joint Staff, the Services, the Defense Information Systems Agency (DISA), US Cyber Command (USCC), and other DoD agencies in planning, synchronizing, and implementing actions to enable the Department to achieve JIE. The JIE effort was initiated based on the Commander, USCC's November 2011 brief to the Joint Chiefs of Staff on the risk associated with the inability to "see," protect, and defend the entire DoD network and made recommendations to consolidate IT infrastructure for achieving improved effectiveness. Our primary goals are to make the Department more effective and more secure against cyber threats and vulnerabilities. A secondary, but very important goal is to reduce the cost associated with the Department's overall information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure at the enterprise level.

A team consisting of experts from across the DoD is currently working through the technical, operations, and governance approaches to develop an implementation plan of action and milestones, and associated cost estimates that will replace the current Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap (DoD ITESR) (Version 1.0 dated 6 September 2011). We are using the intelligence community's information technology effectiveness modernization efforts to inform the JIE planning. The initial DoD ITESR consolidation initiatives represented ongoing activities that the DoD CIO identified in coordination with the Services. The validation of these initial activities permitted the Services to focus their limited resources on implementing the following eight near term initiatives (Consolidate Security Infrastructure, Implement Cross-Domain Solution as an Enterprise Service, Joint Information Environment (JIE)/Joint Enterprise Network (JEN), Data Center and Server Consolidation, Enterprise Messaging and Collaboration (including Email), Identity and Access Management (IdAM) Services, Consolidate Software Purchasing, and Consolidate Hardware Purchasing). In the DoD ITESR these initiatives across the Services were optimized at the Services' levels. The overall JIE approach is to further optimize the IT normalization to the DoD and Joint levels.

The ultimate beneficiary of JIE is the commander in the field, allowing for more innovative integration of information technologies, operations, and cyber security at a tempo more appropriate to today's fast-paced operational conditions. Specific benefits include:

- A standardized information and security architecture will improve how DoD operates and secures its networks on a global level. Users and systems will be able to trust their connection from end to end with the assurance that their activity will not be compromised.

- The JIE's standard security architecture will enable cyber operators at every level to see the status of their networks for operations and security and enable commonality in how cyber threats are countered. The Department will know who is operating on its networks and what they are doing, and be able to attribute their actions with a high degree of confidence. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk.

- Consolidation of data centers, operations centers and help desks will enable users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location.

- A consistent DoD-wide IT architecture supports effective fielding of Department capabilities in support of information sharing, as well as sustainment and integration of legacy systems.

The Department will have to make the required investments to effect the transition from the Department's as-is environment to the desired to-be state. The JIE will be operated and managed per the Unified Command Plan (UCP) using enforceable standards, specification, and common tactics techniques & procedures (TTPs). The JIE framework of IT capabilities and processes will ultimately result in a secure, joint information environment comprised of shared IT infrastructure, enterprise services, and a single security architecture.

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

Information as a Strategic Asset

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.

Major enabling objectives:

- Increase Information Availability
- Broaden Enterprise Services
- Build Community-based Solutions
- Leverage Pilots and Experimentation
- Strengthen Information

Interoperable Infrastructure

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.

Major enabling objectives:

- Shared Computing Resources
- Dynamic NetOps
- Increase Transmission Capability
- Enhanced Communications Interfaces
- Protect DoD Internet Equities

Synchronized and Responsive Ops

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

Major enabling objectives:

- Manage NetOps Risk
- IE Situational Awareness and Management
- Aligned NetOps Policies and Standards

Cybersecurity

DoD can accomplish its missions in the face of cyber warfare by a capable adversary.

Major enabling objectives:

- Resilience to operate through cyber attacks
- Agile, safe information sharing with mission partners
- Robust attack detection diagnosis and response
- Information security

Optimizing IT Investments

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.

Agile IM/IT/IA Workforce

An agile IM/IT/IA workforce able to dynamically operate, defend, and advance the Defense Information Enterprise.

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.

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 Consolidation (DCC) which is consistent with the Federal Data Center Consolidation Initiative (FDCCI). DoD Components are considering all options for achieving consolidation that includes infrastructure consolidation, virtualization and cloud computing, operational efficiencies, and application rationalization to name a few. The current DoD goal is to reduce data centers by 575 by the end of FY15. DoD has confirmed the closure of 64 data centers in FY12. DoD continues to identify additional data centers for closure and is aggressively pursuing consolidation and virtualization. Based on the latest quarterly data center closure tracking, the DoD has projected the closing of 269 data centers in FY13 and 54 data centers in FY14. These projected FY13 and FY14 closures result in projected savings of $583 million dollars.

DOD DCC Savings Summary (FY11 - FY14)

($TY BY13)

Summary Metrics	FY11 (5)	FY12	FY13 (6)	FY14
Data Center Closures # (1) (2)	55	64	269	54
Total Impacted Servers	3400 (4)	4,072	14,794	4,420
Annual Projected Savings (3)	$88,579,251	$100,190,560	$474,616,287	$108,861,613
Cumulative Realized Savings	$0	$88,579,251	$188,769,811	$663,386,098

Notes:

1) Figures represent data center closure records in DoD's FY13 Q1 dataset

2) Captures valid records in DoD's inventory and records "accepted" by the OMB TCO Model

3) Savings are realized fiscal year after closure year

4) Reflects incomplete dataset from OMB TCO model for FY11 closures

5) FY11 savings based on average inflation adjusted server costs of FY12 thru FY14 due to cost data gaps in OMB TCO model for FY11

6) Reflects 13 sites that had target closure dates in FY12, but were not listed as closed in Q1 data

The Department recently compiled a global inventory of its data centers, and is establishing four classes of data centers to assist in the development and execution of our data center consolidation strategy. These four types of data centers are:

- Core Data Center (CDC) – delivers enterprise services and provides primary migration point for systems and applications; these are our most important data centers, strategically located to provide speed of access to global information requirements;

- Installation Processing Node (IPN) – provides local services to DoD installations and hosting systems not suited for CDCs, these will be located at the installation level, and will consolidate the duplicative data centers at the installations;

- Special Purpose Processing Node (SPPN) – provides compute and storage for fixed infrastructure or facilities, such as test ranges, labs, medical diagnostic equipment, and machine shops.

- Tactical/Mobile Processing Node (TPN) – provides support to the deployed warfighter at the tactical edge; these unique "data centers" directly support the warfighter in a disadvantaged or tactical environment, but connect back into the Generating Force information sources and core data centers.

The DoD Core Data Center Reference Architecture was published in October 2012 and provides the foundation for the DoD's data center consolidation efforts as well as supports the emerging Department's Cloud Computing capability, which will be "tied" to data centers.

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.

Enterprise Services

Enterprise services are those global applications that can be used by many, if not all users within DoD. They are a key element of achieving more effective operations and improved security across the Department. An example of what the Department is doing in this area is Defense Enterprise Email, which is an enterprise messaging tool, built by consolidating existing disparate email servers into a global capable server and operated by DISA on a fee-for-service basis, which provides DoD with a common enterprise directory service and a consolidated email service.

The enterprise directory service is being incorporated by many organizations, and the Defense Enterprise Email is currently used by DISA, EUCOM, AFRICOM, USFK, Defense Manpower Data Center, Office of Naval Research, Navy Recruiting Command, the Joint Staff, and the US Army. As of March 2013, there are 976,000 enterprise email users on the Department's unclassified network and 21,000 users on the DoD Secret network, and continued adoption and consolidation to this capability is expected in the future.

In June 2012, we completed a report to Congress stating that decisions to consolidate organizational email capabilities beyond the current user community, such as Navy, Marine Corps and Air Force, are being considered and will be validated using a business case analysis.

Cloud Computing

Cloud Computing is becoming a critical component of the JIE efforts and will enable users the access to data anywhere, anytime on any approved device. One key objective is to drive the delivery and adoption of a secure, dependable, resilient multi-provider enterprise cloud computing environment that will enhance mission effectiveness and improve IT efficiencies. Cloud services will enhance warfighter mobility by providing secure access to mission data and enterprise services regardless of where the user is located and what device he or she uses.

We recently issued the DoD Cloud Computing Strategy to provide an approach to move the Department to an end state that is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. There are two key components of the Department's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DoD activities in unclassified and classified environments. The second is the Department's adoption of commercial cloud services that can meet the Departments cybersecurity needs while providing capabilities that are at least as effective and efficient as those provided internally.

The DoD's Enterprise cloud infrastructure will provide shared technology capabilities for the consolidation of stovepiped services at installations and in core datacenters. It also will define connectivity standards for end-user devices, unmanned clients and other networks. This will enable the Department to develop and deliver new and more integrated enterprise information services that support our warfighters and business support operations, which will improve the effectiveness, security and reliability of those operations.

The DoD CIO continues to investigate new ways to leverage commercial cloud computing innovations and efficiencies to improve the Department. The nature of the Department's mission, and the risk to national security if DoD information were to be compromised, requires the careful evaluation of commercial cloud services, especially in areas of information assurance (IA) and cybersecurity, continuity of operations, and resilience. To improve our cybersecurity posture with regards to commercial cloud computing, we are participating in the Federal Risk Authorization and Management Program (FedRAMP) and updating our own cybersecurity policies.

I have designated DISA as the DoD Enterprise Cloud Service Broker to facilitate and optimize access and use of commercial cloud services that can meet DoD's security and interoperability requirements, and ensure that new services are not duplicative of others within the Department while consolidating cloud service demand at an enterprise level. In addition, DISA, as the DoD broker, will leverage the FedRAMP standardized security authorization process, including the accepted minimum security baseline for low and moderate services, and ongoing continuous monitoring to ensure that appropriate security controls remain in place and are functioning properly.

Cyberspace Operations

In recognition of cyberspace as an operational domain and the emerging mission to Defend the Nation against cyber threats as directed by the President, this year's budget provides funds to increase defensive capabilities and develop the cyber Joint Force under a new force planning model.

The unique attributes of cyberspace operations require trained and ready cyberspace forces to detect, deter, and, if directed, respond to threats in cyberspace. Securing and defending cyberspace requires close collaboration among Federal, state and local governments, private sector partners, and allies and partners abroad. This year's budget establishes dedicated cyber teams to execute this mission on Defense Department networks and in support of Combatant Command and national missions.

This budget reflects an emphasis on enhancing our workforce to successfully execute defensive and offensive missions in cyberspace. The Department is implementing a new cyber force planning model that will realign military, civilian and contractor manpower positions (with associated support costs) under U.S. Cyber Command (USCYBERCOM) in a three-year phased build-up beginning in FY 2014. This provides manpower, training and support costs for regional cyber mission teams to be located in Maryland, Texas, Georgia and Hawaii as well as other Combatant Command and military service locations. In addition, manpower at the National Security Agency continues to be funded to provide both cybersecurity and intelligence support to the USCYBERCOM teams. This overall force construct will provide capacity for the "Defend the Nation" mission, the cyber combat mission (in support of Combatant Command needs), and the cyberspace protection mission which defends Defense Department networks.

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.

Agile IT/Cyberspace 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 capabilities to support the business, intelligence and warfighting missions of the Department.

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.

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.

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), 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. 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) implementing emerging portfolio management concepts such as OMB's PortfolioStat within DoD.

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.

Business Service Segments and Defense Business Systems: Commonly referred to as the business mission area, this segment provides direct support to the warfighter through the enabling functions and information systems to support business activities, such as Acquisition, Technology, and Logistics; Financial Management, Personnel and Readiness, Installations and Environment; and Defense Security. The business mission area is aligned to support the warfighter through the Strategic Management Plan (SMP), which is linked to the Quadrennial Defense Review (QDR) by its strategic goals and initiatives. In addition to guiding the business activities of the Department to support the warfighter,

the SMP also articulates changes needed in the business mission area while enabling unity of effort across the enterprise. The current SMP 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

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. Another foundation is the introduction of Functional Strategies developed by the business line owners, known as Principal Staff Assistants (PSAs). Functional Strategies define business outcomes, priorities, measures, and standards. Organizational Execution Plans developed by each Component articulate their planned approach by aligning to and implementing their part of the Functional Strategies. Section 901 of the Fiscal Year 2012 National Defense Authorization Act (FY 2012 NDAA), now codified at title 10, U.S.C §2222, includes significant changes to the requirements for investment review and certification of Defense Business Systems before funds, whether appropriated or non-appropriated, can be available for obligation.. Section 901 also requires the establishment of a single Investment Review Board (IRB) and an investment management process, consistent with section 11312 of Title 40. It expands the scope of systems requiring certification to include any business system with a total cost in excess of $1M over the period of the current future–years defense program, regardless of type of funding or whether any development or modernization is planned. In the prior IRB process, approximately $1.8 billion in funding for defense business system investments was assessed and certified each year. The expanded scope in Section 901 resulted in the assessment of approximately $7B in FY 2013 funds certification requests submitted for business system information technology (IT) solutions. The new legislation requires active participation at most levels across DoD and enables an integrated, portfolio-based approach for the annual evaluation and funds certification of defense business system investments.

When assessing the FY13 certification requests, DoD assessed the amount of funds requested for certification, strategic alignment, utility, and compliance of each system within the broader functional portfolio. When assessing the portfolios, DoD considered the functional strategies developed by the appropriate business line owner (DoD Principal Staff Assistant (PSA)) and then analyzed the portfolio more broadly against other investments in the Department and against the overarching DoD priorities and lessons learned from previous business system investments. This new investment management approach allows for an expansive and thorough look at how investments within a given functional or organizational portfolio fit and help to enable smart investment decisions that align to mission priorities. The process focuses on DoD Components taking responsibility for

reviewing and aligning all business system investments within their Component prior to bringing their plans to the Defense Business Council (DBC), which is the governing body that reviews the proposed investments.

As the new IRB process stabilizes and matures, the business mission area will more directly link the certification decisions to the budget process by reviewing and providing certification decisions earlier in the budget cycle to allow changes to the budget submissions based on certification outcomes.

Looking at FY2014 and beyond, the business mission area recognizes that it must transform its business operations in order to meet today's business challenges. The business mission area has established a set of "guiding principles" to inform strategy and operations for the years ahead. These guiding principles include (1) the need for a cost culture, (2) effective data management and analytics, (3) continued modernization and rationalization of business systems and, (4) improved business alignment. These four cross-cutting principles will help guide DoD as it executes its strategic vision for business operations. The influence of these guiding principles as we execute our initiatives in support of our goals enables us to gain value from our actions and will form the backbone of the Department's 21st century business operations.

Internalizing a cost culture is highly relevant to the DoD IT budget. With at least $500 billion in DoD-wide budget cuts to be absorbed over the next 10 years, we have been asked to "do more without more." Without the support of a growing budget, instilling a strong cost culture across the department will be critical to enabling the business mission area to continue to deliver value to the warfighter. This culture of accurately estimating, capturing and analyzing costs, and delivering our products and services at or below targeted costs will help us not only meet our budget mandates, but also enable the business mission area to operate like the twenty-first century business enterprise that we aspire to be. We will use cost analyses to inform where we will invest and how we will manage our business operations in order to provide high value to the warfighter at an affordable cost. This approach will be used across the business mission area and applies to IT investments as well.

Effective data management and analytics will be a core competency in our cost culture. The business mission area will build capacity to manage the data available and require that investment, acquisition and management decisions are made with full consideration of relevant data sources. Some reports estimate that the amount of business data produced in the world is doubling every few years or even faster. This data, or information, can be a critical asset to the Department, especially given the fiscal challenges we now face. In industry, we have observed that those organizations who harness the power of the data to make decisions can outperform those that do not. Using industry as a guide, we believe that using data effectively to make decisions can have an even greater impact on our ability to deliver value to the warfighter than hiring more people or investing more in information technology solutions.

Our desire to make decisions informed by data is applicable to all parts of the business mission area, and it is especially relevant as we work to modernize and rationalize our defense business systems portfolio. Our knowledge and experience in this space tells us that there are opportunities to both modernize and rationalize our business systems to achieve more efficient and effective operations. Unintentional business system redundancies drain the department of increasingly scarce resources, can create interoperability and data challenges, and can inhibit our ability to efficiently support the warfighter. A focus on cost effective investments in business solutions that provide timely and accurate data for decision making also enables the achievement of our business goals. Informed business system modernization and rationalization will also enable the realization of the expected value of our newer business systems, including ERPs. For The Department's investment review process we have been able to use data as an input to business system modernization and rationalization decision making.

Enabling business alignment of our strategy with our operations across the Military Components and Defense Agencies will improve performance while reducing redundancies and overlaps is another key guiding principle for our operations. In addition to communicating our strategy to shape the daily operations across our organization, we must measure our performance to assess progress toward achievement of our goals and strategy. If we fall short, we will reassess our priorities and resource allocations. Aligning our strategy to our operations across the Military Components and Defense Agencies will also require top-down support for our goals Committing to the accomplishment of this strategy and aligning each organization to achieve these common goals is paramount and requires both transformation and the break-down of many siloed processes, approaches, and views of the business mission area.

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, C4/Cyber Operations & Defense Review Board, Enterprise Architecture & Services Review Board, and the Information Resources Management Investment Review Board which serve as senior forums in the Department. They are responsible for guiding and oversight of enterprise-wide IT solution security, design, and investment. 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 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 contributions[1] in FY 2014.

(Funding identified in actual dollars)

Initiative	FY13	FY14
Financial Management LoB	$202,173	$187,342
Human Resources Management LoB	$260,870	$260,870
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
Performance Management LoB[2]	$2,795,000	$2,580,000
DoD Total	**$5,499,043**	**$5,534,212**

Objective of eGovernment Initiatives[3]:

Financial Management LoB / Managing Partner, General Services Administration - The Financial Management Line of Business vision is to create government-wide financial management solutions that are efficient and improve business performance while ensuring integrity in accountability, financial controls, and mission effectiveness. FM LoB is working in coordination with the Chief Financial Officer's Council (CFOC), the Council on Financial Assistance Reform (COFAR), and partner agencies to bring together the financial management and financial assistance communities to achieve this vision, improve transparency of federal spending, and streamline agency operations.

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

[1] 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.
[2] New program for DoD as directed by OMB.
[3] OMB Report to Congress on the benefits of the President's E-Government Initiatives for Fiscal Year 2013.

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.

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 – Within the Department of Defense, geospatially enabling traditional business data has improved business process efficiency, allowed for geographically based analytic and investment processes, improved infrastructure asset tracking, improved mission delivery, and promoted the use of business intelligence in the Department's decision support systems.

Budget 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.

Performance Management Line of Business / Managing Partner, General Services Administration – The Performance Management Line of Business is an interagency effort to develop government-wide performance management capabilities and meet the transparency requirements of the GPRA Modernization Act. Performance information will be reported through a Federal website, which includes advanced data display and reporting capabilities, the ability to extract raw data, and over time will integrate other government –wide data such as program, human capital and spending information.

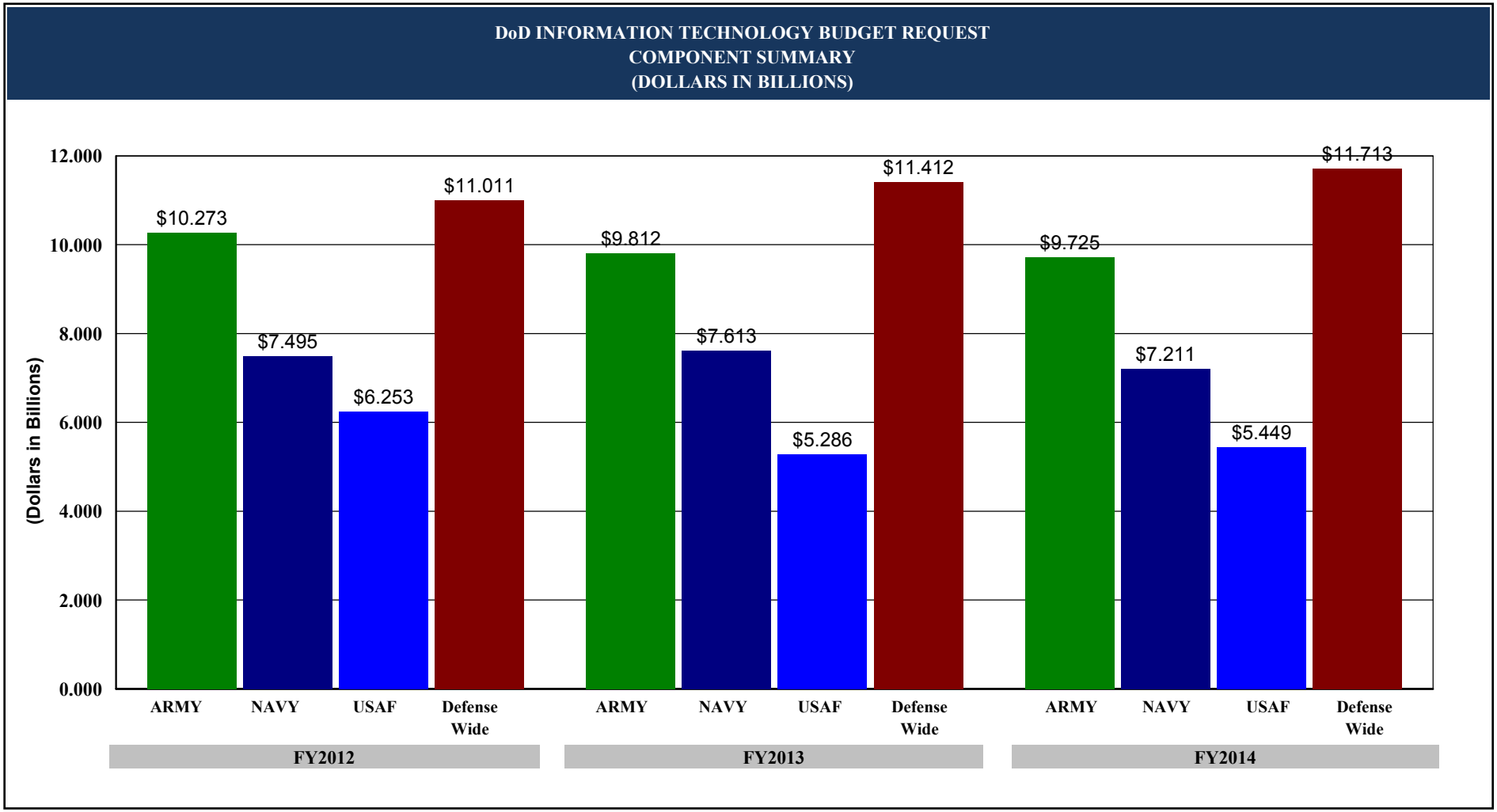
Notes:

The FY2013 Department of Defense IT Budget materials are available on the web at: https://snap.pae.osd.mil/snapit/BudgetDocs2014.aspx

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

DEPARTMENT	FY2012	FY2013	FY2014
DEPARTMENT OF ARMY	$10,273.039	$9,811.701	$9,725.381
DEPARTMENT OF NAVY	$7,495.064	$7,613.270	$7,210.651
DEPARTMENT OF AIR FORCE	$6,252.871	$5,285.742	$5,449.284
DEFENSE WIDE ACTIVITIES	$11,011.159	$11,412.301	$11,713.205
DOD TOTALS	**$35,032.133**	**$34,123.014**	**$34,098.521**

Page left intentionally blank


DoD INFORMATION TECHNOLOGY BUDGET REQUEST
COMPONENT SUMMARY
(DOLLARS IN BILLIONS)
(Dollars in Billions)
12.000
10.000
8.000
6.000
4.000
2.000
0.000
$10.273
$7.495
$6.253
$11.011
$9.812
$7.613
$5.286
$11.412
$9.725
$7.211
$5.449
$11.713
ARMY
NAVY
USAF
Defense Wide
FY2012
FY2013
FY2014

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY COMPONENT (DOLLARS IN MILLIONS)			
	FY2012	FY2013	FY2014
GRAND TOTAL	**$35,032.133**	**$34,123.014**	**$34,098.521**
DEPARTMENTS	**$24,020.974**	**$22,710.713**	**$22,385.316**
ARMY	$10,273.039	$9,811.701	$9,725.381
NAVY	$7,495.064	$7,613.270	$7,210.651
USAF	$6,252.871	$5,285.742	$5,449.284
DEFENSE AGENCIES	**$8,136.555**	**$8,682.938**	**$8,791.183**
DARPA	$32.937	$33.984	$35.003
DCAA	$28.869	$29.358	$29.491
DCMA	$159.825	$129.492	$133.858
DeCA	$96.130	$95.469	$100.834
DFAS	$384.217	$415.651	$383.073
DISA	$4,795.869	$5,158.371	$5,377.094
DLA	$1,166.618	$1,269.907	$1,233.368
DSCA	$0.971	$3.709	$18.221
DSS	$32.205	$39.408	$33.959
DTRA	$148.189	$124.161	$122.644
DTSA	$4.849	$5.599	$5.694
JCS	$114.449	$119.726	$115.814
MDA	$165.440	$151.236	$160.613
OSD	$28.445	$24.159	$23.911
PFPA	$17.790	$18.812	$20.650
SOCOM	$459.938	$477.237	$422.414
TRANSCOM	$451.309	$528.540	$517.509
USD(AT&L)	$48.505	$58.119	$57.033
FIELD ACTIVITIES	**$2,874.604**	**$2,729.363**	**$2,922.022**
DCMO	$9.855	$8.842	$9.811

BY COMPONENT - continued (DOLLARS IN MILLIONS)			
	FY2011	**FY2012**	**FY2013**
DHRA	$281.566	$296.413	$371.369
DMACT	$9.586	$24.953	$24.846
DODDE	$87.409	$88.743	$90.311
DPMO	$4.000	$3.600	$3.200
DTIC	$19.583	$19.083	$22.052
IG	$46.139	$46.140	$37.944
NDU	$18.223	$16.309	$16.309
OSDPR	$10.458	$14.167	$13.829
TMA	$2,176.022	$1,990.826	$2,084.562
WHS	$211.763	$220.287	$247.789

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

SEGMENT	FY2012	FY2013	FY2014
ACQUISITION	$394.993	$457.810	$463.644
BATTLESPACE AWARENESS-ENVIRONMENT	$391.421	$368.521	$459.445
BATTLESPACE AWARENESS-ISR	$85.124	$50.171	$96.436
BATTLESPACE NETWORKS	$4,399.907	$4,217.769	$4,073.833
BUILDING PARTNERSHIPS	$3.603	$7.342	$21.004
BUSINESS SERVICES TBD	$149.857	$104.606	$97.161
COMMAND & CONTROL	$2,491.343	$2,371.909	$2,264.893
CORE MISSION TBD	$234.737	$212.637	$223.564
DOD IT INFRASTRUCTURE	$18,247.203	$17,229.760	$17,167.633
ENTERPRISE SERVICES TBD	$148.447	$244.817	$432.198
FINANCIAL MANAGEMENT	$758.494	$858.533	$837.410
FORCE APPLICATION	$945.150	$754.557	$895.058
FORCE MANAGEMENT	$94.512	$64.900	$168.544
FORCE TRAINING	$268.637	$289.825	$330.455
HEALTH	$1,247.726	$1,142.695	$1,155.849
HUMAN RESOURCE MANAGEMENT	$1,612.346	$1,821.682	$1,883.046
INSTALLATION SUPPORT	$147.657	$191.710	$192.102
IT MANAGEMENT	$668.092	$557.878	$517.548
LOGISTICS/SUPPLY CHAIN MANAGEMENT	$2,445.464	$2,796.470	$2,561.872
PROTECTION	$297.420	$379.422	$256.826
DOD TOTALS	**35,032.133**	**34,123.014**	**34,098.521**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST SEGMENTS BY COMPONENT (DOLLARS IN MILLIONS)			
ACQUISITION	**FY2012**	**FY2013**	**FY2014**
ARMY	$43.973	$60.870	$79.847
NAVY	$173.410	$190.345	$177.678
AIR FORCE	$61.137	$81.000	$71.190
DEFENSE WIDE	$116.473	$125.595	$134.929
	$394.993	$ 457.810	$ 463.644
BATTLESPACE AWARENESS-ENVIRONMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$255.692	$242.176	$309.218
NAVY	$87.062	$65.005	$73.541
AIR FORCE	$48.667	$61.340	$76.686
	$391.421	$ 368.521	$ 459.445
BATTLESPACE AWARENESS-ISR	**FY2012**	**FY2013**	**FY2014**
NAVY	$85.124	$50.171	$96.436
	$85.124	$ 50.171	$ 96.436
BATTLESPACE NETWORKS	**FY2012**	**FY2013**	**FY2014**
ARMY	$2,036.106	$2,018.251	$2,184.207
NAVY	$1,089.363	$981.550	$715.949
AIR FORCE	$603.504	$582.481	$493.295
DEFENSE WIDE	$670.934	$635.487	$680.382
	$4,399.907	$ 4,217.769	$ 4,073.833
BUILDING PARTNERSHIPS	**FY2012**	**FY2013**	**FY2014**
AIR FORCE	$1.767	$1.520	$1.612
DEFENSE WIDE	$1.836	$5.822	$19.392
	$3.603	$ 7.342	$ 21.004
BUSINESS SERVICES TBD	**FY2012**	**FY2013**	**FY2014**
ARMY	$2.915	$2.732	$0.950
NAVY	$127.062	$85.433	$72.411
AIR FORCE	$5.097	$1.258	$7.596
DEFENSE WIDE	$14.783	$15.183	$16.204
	$149.857	$ 104.606	$ 97.161

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
COMMAND & CONTROL	**FY2012**	**FY2013**	**FY2014**
ARMY	$422.502	$329.493	$261.806
NAVY	$474.134	$520.096	$509.197
AIR FORCE	$1,000.970	$913.755	$897.984
DEFENSE WIDE	$593.737	$608.565	$595.906
	$2,491.343	$ 2,371.909	$ 2,264.893
CORE MISSION TBD	**FY2012**	**FY2013**	**FY2014**
ARMY	$44.100	$57.974	$78.621
NAVY	$0.052	$0.000	$0.000
AIR FORCE	$188.436	$152.072	$142.308
DEFENSE WIDE	$2.149	$2.591	$2.635
	$234.737	$ 212.637	$ 223.564
DOD IT INFRASTRUCTURE	**FY2012**	**FY2013**	**FY2014**
ARMY	$5,087.187	$4,297.404	$4,199.810
NAVY	$3,690.157	$3,860.348	$3,737.164
AIR FORCE	$3,135.388	$2,333.017	$2,231.257
DEFENSE WIDE	$6,334.471	$6,738.991	$6,999.402
	$18,247.203	$ 17,229.760	$ 17,167.633
ENTERPRISE SERVICES TBD	**FY2012**	**FY2013**	**FY2014**
ARMY	$47.247	$117.366	$126.244
NAVY	$30.329	$108.255	$168.471
AIR FORCE	$70.071	$15.725	$135.449
DEFENSE WIDE	$0.800	$3.471	$2.034
	$148.447	$ 244.817	$ 432.198
FINANCIAL MANAGEMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$156.962	$153.714	$144.972
NAVY	$120.568	$159.269	$118.807
AIR FORCE	$136.320	$159.918	$192.252
DEFENSE WIDE	$344.644	$385.632	$381.379
	$758.494	$ 858.533	$ 837.410

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
FORCE APPLICATION	**FY2012**	**FY2013**	**FY2014**
ARMY	$518.164	$385.610	$328.171
NAVY	$106.024	$170.662	$242.429
AIR FORCE	$295.255	$158.858	$300.605
DEFENSE WIDE	$25.707	$39.427	$23.853
	$945.150	$ 754.557	$ 895.058
FORCE MANAGEMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$16.538	$5.561	$4.693
NAVY	$21.145	$18.268	$21.457
AIR FORCE	$29.989	$5.954	$115.834
DEFENCE WIDE	$10.458	$14.167	$13.829
DEFENSE WIDE	$16.382	$20.950	$12.731
	$94.512	$ 64.900	$ 168.544
FORCE TRAINING	**FY2012**	**FY2013**	**FY2014**
ARMY	$207.632	$258.161	$275.026
NAVY	$17.220	$13.707	$14.572
AIR FORCE	$23.827	$9.828	$23.309
DEFENSE WIDE	$19.958	$8.129	$17.548
	$268.637	$ 289.825	$ 330.455
HEALTH	**FY2012**	**FY2013**	**FY2014**
ARMY	$5.523	$10.113	$7.224
NAVY	$3.245	$3.260	$3.341
AIR FORCE	$0.750	$0.750	$0.550
DEFENSE WIDE	$1,238.208	$1,128.572	$1,144.734
	$1,247.726	$ 1,142.695	$ 1,155.849
HUMAN RESOURCE MANAGEMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$521.386	$680.935	$685.230
NAVY	$447.390	$417.681	$438.907
AIR FORCE	$207.498	$241.733	$230.187
DEFENSE WIDE	$436.072	$481.333	$528.722
	$1,612.346	$ 1,821.682	$ 1,883.046

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
INSTALLATION SUPPORT	**FY2012**	**FY2013**	**FY2014**
ARMY	$56.441	$67.894	$62.907
NAVY	$34.170	$40.526	$42.880
AIR FORCE	$50.312	$72.876	$76.276
DEFENSE WIDE	$6.734	$10.414	$10.039
	$147.657	$ 191.710	$ 192.102
IT MANAGEMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$67.491	$45.561	$33.761
NAVY	$17.913	$45.189	$49.442
AIR FORCE	$62.694	$31.852	$54.120
DEFENSE WIDE	$519.994	$435.276	$380.225
	$668.092	$ 557.878	$ 517.548
LOGISTICS/SUPPLY CHAIN MANAGEMENT	**FY2012**	**FY2013**	**FY2014**
ARMY	$621.294	$846.655	$801.186
NAVY	$932.136	$839.590	$698.487
AIR FORCE	$298.936	$422.503	$373.714
DEFENSE WIDE	$593.098	$687.722	$688.485
	$2,445.464	$ 2,796.470	$ 2,561.872
PROTECTION	**FY2012**	**FY2013**	**FY2014**
ARMY	$161.886	$231.231	$141.508
NAVY	$38.560	$43.915	$29.482
AIR FORCE	$32.253	$39.302	$25.060
DEFENSE WIDE	$64.721	$64.974	$60.776
	$297.420	$ 379.422	$ 256.826
DoD Totals	**$35,032.133**	**$34,123.014**	**$34,098.521**

Page left intentionally blank

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

MISSION AREA	FY2012	FY2013	FY2014
BUSINESS	$6,756.537	$7,373.506	$7,191.084
DEFENSE INTELLIGENCE	$85.124	$50.171	$96.436
ENTERPRISE INFORMATION ENVIRONMENT	$19,063.742	$18,032.455	$18,117.379
WARFIGHTING	$9,126.730	$8,666.882	$8,693.622
DOD TOTALS	**$35,032.133**	**$34,123.014**	**$34,098.521**

Page left intentionally blank