Department of Defense
Information Technology
Budget Exhibit
Overview

Fiscal Year 2017
President's
Budget Request

March 2016

Preparation of this study/report*
Cost the Department of Defense a
Total of approximately $1,900,300 for
The 2016 Fiscal Year

*Includes unclassified report and its
classified annex

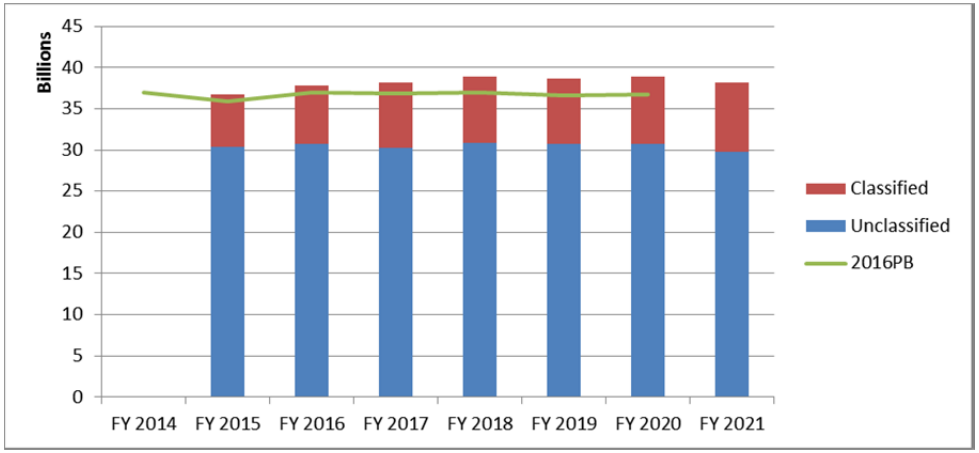
Department of Defense
Fiscal Year (FY) 2017 IT President's Budget Request

Table of Contents
FY17 President's IT Budget Submission

Department of Defense
Fiscal Year (FY) 2017 IT President's Budget Request

1. Introduction (DoD IT Budget Overview)

The Department of Defense (DoD) fiscal year 2017 total Information Technology (IT) Budget Request is $38.2B, which includes both unclassified ($30.3B) and classified ($7.9B) investments. This represents a $0.4B (1%) increase from the fiscal year 2016 enacted budget. The bedrock of this gain is an increase of $0.9B for funding the classified Cyberspace Operations programs supporting the Cyber Mission Forces and other Cyberspace Activities. Consistent with Administration guidance, the DoD IT Budget remains relatively constant throughout the FY17 - FY21 Future Year Defense Plan (FYDP); factoring in the future value of money DoD projects approximately $3.5B in decreased IT spending within the FYDP. The DoD's classified IT budget request includes cyberspace operations investments and other classified IT investments, and is projected to increase at about twice the rate of inflation over the FYDP. Funding trends in the classified and unclassified budgets over the FYDP are shown in the below chart.



A mission critical resource, DoD networks underpin Information Operations, Command and Control, logistics, finance, transportation, medical, maintenance and other activities. The Department's evolving IT modernization efforts, envisioned in the concept known as the Joint Information Environment (JIE), represent a critical way in which DoD is improving its IT security, efficiency, and effectiveness. JIE will improve alignment of networks and systems, enabling and empowering our military through a shared IT infrastructure with common configurations and management, and a common set of enterprise services within a single security architecture. A top priority to achieve JIE is the Joint Regional Security Stacks (JRSS), which improve cybersecurity and cyber situational awareness by shrinking the attack surface from more than 1,000 disparate ingress points to about fifty, achieving standard network security architecture, and addressing the immediate need to defend the cyber warfighting domain. The DoD Chief Information Officer (DoD CIO) oversees the planning, synchronization, and implementation actions that will help achieve JIE with the Joint Staff, the Military Services, the Defense Information Systems Agency, U.S. Cyber Command, and other DoD Components.

The United States and its international partner's face a world of complex national security challenges, and the Department's IT remains increasingly at the forefront of these complex challenges. As the Secretary of Defense remarked at the Economic Club of Washington on February 2nd of 2016 while previewing the 2017 defense budget, today's security environment is dramatically different than the environment in which we have engaged for the last twenty-five years, and it requires new ways of thinking and acting. Taking the long view, the Department is driving smart and essential technological innovation in the budget to stay ahead of future threats over far into the future and keep the U.S. military the best in the world. From the perspective of the DoD IT budget and the Department's IT priorities, nowhere is this more apparent than in cyberspace. As Secretary Carter explained, fiscal year 2017 investments in cybersecurity

totaling nearly $7 billion will help further improve DoD's network defenses, build more training ranges for the Department's cyber warriors, and develop the cyber tools and infrastructure needed to provide offensive cyber operations. The DoD's Cyberspace Operations and Information Assurance budget is a collection of efforts intended to operate, defend, and secure the information networks. A copy of this FY17 classified IT annex can be obtained by contacting the office of the DoD CIO or via the link in the section of this overview about the classified IT budget submission (#5). The below chart summarizes the DoD classified and unclassified IT budget requests for each of the Military Departments and DoD Components over the FYDP.

(Dollars in Thousands)

	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021
ARMY							
Unclassified	$ 8,650,985	$ 8,269,274	$ 8,018,146	$ 8,618,550	$ 8,681,576	$ 8,484,400	$ 7,833,753
Classified	$ 961,508	$ 1,452,727	$ 1,767,895	$ 1,758,788	$ 1,797,117	$ 1,890,847	$ 1,872,601
Subtotal	$ 9,612,493	$ 9,722,001	$ 9,786,041	$ 10,377,338	$ 10,478,693	$ 10,375,247	$ 9,706,354
NAVY							
Unclassified	$ 6,547,940	$ 6,980,128	$ 6,816,067	$ 6,812,052	$ 6,937,244	$ 7,058,879	$ 6,842,414
Classified	$ 913,509	$ 1,050,012	$ 1,154,988	$ 1,216,298	$ 1,194,690	$ 1,205,234	$ 1,222,386
Subtotal	$ 7,461,449	$ 8,030,140	$ 7,971,055	$ 8,028,350	$ 8,131,934	$ 8,264,113	$ 8,064,800
AIR FORCE							
Unclassified	$ 6,174,968	$ 5,665,974	$ 5,597,831	$ 5,337,021	$ 4,829,865	$ 4,991,634	$ 4,805,479
Classified	$ 1,627,057	$ 1,652,041	$ 1,990,531	$ 2,119,187	$ 1,998,849	$ 1,995,222	$ 2,043,884
Subtotal	$ 7,802,025	$ 7,318,015	$ 7,588,362	$ 7,456,208	$ 6,828,714	$ 6,986,856	$ 6,849,363
Defense Wide							
Unclassified	$ 9,040,379	$ 9,864,869	$ 9,865,140	$ 10,127,900	$ 10,301,063	$10,255,575	$10,294,585
Classified	$ 2,807,842	$ 2,856,414	$ 2,945,638	$ 2,963,682	$ 2,950,439	$ 2,978,839	$ 3,270,961
Subtotal	$ 11,848,221	$ 12,721,283	$ 12,810,778	$ 13,091,582	$ 13,251,502	$ 13,234,414	$ 13,565,546
Total							
Unclassified	$ 30,414,272	$ 30,780,245	$ 30,297,184	$ 30,895,523	$ 30,749,748	$ 30,790,488	$ 29,776,231
Classified	$ 6,309,916	$ 7,011,194	$ 7,859,052	$ 8,057,955	$ 7,941,095	$ 8,070,142	$ 8,409,832
Total	$ 36,724,188	$ 37,791,439	$ 38,156,236	$ 38,953,478	$ 38,690,843	$ 38,860,630	$ 38,186,063

2. DoD IT Priorities

A. Modernize the Networks

The Department's IT networks and systems are complicated. They have evolved over many years; support military efforts on all seven continents; and empower different Military Services that operate like their own autonomous and enormous corporations, each with its own budget, constituencies, and priorities. The concept of modernizing and integrating all networks and systems to help ensure efficient, effective, secure information sharing with the DoD's internal and external partners is called JIE. As an important conceptual IT modernization effort, work toward a complete JIE end state will never cease. In short, JIE will drive a more secure, more effective, and more efficient IT environment for DoD.

The JIE framework comprises a number of discrete, but related, elements that when integrated will more securely provide the Department with IT capabilities such as computing and information storage, transfer, and sharing. DoD's top priority to enable the JIE is JRSS. Today, DoD has approximately 1,000 disparate security suites facilitated by separate, individualized, localized Service and Agency systems, and more than 5,000 firewalls. Transitioning to the regionally based, centrally managed suite of security appliances, known as JRSS will simplify and secure this environment and significantly reduce DoD's "attack surface" to fewer than fifty points on the network. In addition, JRSS will increase cyber situational awareness, reduce costs, improve configuration management, and advance functionality across the network.

To improve cyber situational awareness, JRSS will be the baseline for more coherent, singular security architecture for DoD's cyber defenders. By normalizing security for data and networks across the Services, and consolidating the Department's security posture across its infrastructure, JRSS will also enable better data and a central view of the cyber environment and improve the capacity for immediate action and predictive planning. The Deputy Director of United States Cyber Command (CYBERCOM), Lt. Gen. James McLaughlin, has said that achieving cybersecurity will require visibility across all of the Department's networks. JRSS is critical to accomplishing this visibility and advancing cyber situational awareness.

JRSS focuses on three top initiatives. The first is Network Infrastructure Modernization, such as multiprotocol label switching (MPLS) routers and optical transport upgrades, which will accelerate network traffic flow and increase network capacity. The second is a Cybersecurity Reference Architecture, which includes Internet Access Points, Cloud Access Points, and Cyber Situational Awareness Capabilities. This will help General McLaughlin with the across-the-network visibility that his team needs at CYBERCOM. This architecture will set stronger security standards for the stacks – including endpoint security; address the immediate need to defend the cyber warfighting domain; standardize the network security architecture; enable global synchronized network operations by fielding of JRSS suite; and accelerate establishing a standard Command and Control (C2) platform. Third, JRSS includes Enterprise Operations, which focuses on establishing regional operations centers and their associated procedures, and a global operations center to defend the Department's information network.

B. Share with Mission Partners

Coalition communications is an area of critical concern for the Combatant Commanders. The Department regularly works with expected and unexpected mission partners in a range of scenarios. DoD partnered with China and Cuba to provide disaster relief in Haiti, and works with myriad international partners to help defeat ISIL and train partner nations. The need to securely, reliably, affordably share information with all of the partners a mission requires has increased exponentially over time, and it likely will only continue on this same course.

To support this need to securely share information with mission partners – both expected and unexpected – DoD is working to implement a commercially based, robust mission partner environment or system known as the Mission Partner Environment – Information System (MPE-IS). This approach will provide a more cost-effective, rapidly reconfigurable and secure data protection network. MPE will provide full information sharing capability to support

operations in all environments. This will give our Combatant Commanders the flexibility that they need to rapidly add and subtract mission partners as the mission requires, safely, reliably, affordably sharing the data with them that they need to complete the mission, but securely separating the information that needs to stay offline, or making it available to a separate set of mission partners. This will enable sharing with to those who need it, when they need it, where they need it.

The MPE-IS will help DoD extend its enterprise to improve information sharing with mission partners without added equipment, expensive investments, or additional expenses. DoD is coordinating with NATO to ensure that its information-sharing capabilities are complementary. MPE-IS will also strengthen the Department's ability to accommodate unanticipated partners and events in real time, and securely use commercial solutions where appropriate and feasible. When feasible, MPE-IS will also leverage capabilities under the JIE framework such as:

- Identity Management and Access Controls
- Single Security Architecture, providing network boundary defense through firewalls, guards, routers, and other means
- Normalized Network Transport, including MPLS Virtual Private Networks, Common Mission Network Transport, and Commercial Solutions for Classified
- Core Data Centers that provide voice, video, data storage, and application storage

MPE-IS will also include Mission Partner Gateways, providing policies and procedures for partners to "connect" with a mission partner in this coalition communications environment; Joining and Exiting Instructions, with policy and procedures for partners to join; and Cross Domain Solutions, including Trusted Network Environment Cross Domain Solution.

To facilitate secure, reliable, affordable information sharing among mission partners sharing information in this environment, MPE-IS will include communications capabilities such as chat; voice; e-mail with attachments; video, including video teleconferencing; a directory or address list; Web and Web-based file sharing; organizational message service; language translation; file share; Geo-situational awareness; access control; office automation; and print.

C. Manage DoD Data

Leveraging opportunities in the cloud while reducing the Department's physical data-center footprint are enabling DoD to manage its data in a way that improves efficiencies and reduces costs. The Department's key objective in cloud is to deliver a cost efficient, secure-enough enterprise environment – with security driven by the data – that can readily adapt to the DoD mission needs. A robust IT capability built on an integrated set of cloud services provided by both commercial providers and DoD Components is integral to IT modernization efforts.

The Department is pursuing a hybrid approach to cloud that takes advantage of myriad types of cloud solutions will provide the best combination of mission effectiveness and efficiency. This means in some cases, DoD will use a purely commercial solution, while in others DoD will use a modified private cloud hosted in commercial solutions. A DoD private cloud that uses best industry practices will protect the most sensitive data in the cloud.

DoD made significant progress in adoption of commercial cloud services during 2015. To accelerate cloud adoption, the Department updated its cloud policies, published a DoD Cloud Computing Security Requirements Guide, and issued Business Case Analysis guidance requiring DoD Components evaluating new IT investment efforts to consider commercially provided cloud services. As of May 2015, the Department was investing in multiple DoD-provided cloud services affecting millions of users:

Industry partnerships are vital to success, particularly when technology changes rapidly. In January 2015, DoD hosted a cloud industry day open to industry, media, and Federal partners, communicating this new approach to cloud and promoting open dialog with industry. The Department is publishing its

cloud guides in collaboration with industry, producing interactive agility from the commercial and government sector. Industry feedback on this has been positive. DoD is making over 20 investments in commercial cloud services, including: Akamai's Content Delivery Service, Amazon's East/West US Public Cloud, Amazon's Government Community Cloud, Blackboard's Learning Management Cloud, Google Apps for Government, Google Apps for Education, IBM Cloud Services, Microsoft's Office 365 Public Cloud, Microsoft's Office 365 Dedicated ITAR Private Cloud, Oracle's Service Cloud, and Schoology's Learning Management Cloud.

DoD is also working to reduce the cost of its IT across the Department through data center consolidation. DoD is continuing to reduce the number of physical sites and administrators needed to operate its facilities to not only save money, but also to improve security, operate more systems, and reduce the Department's budget by shrinking its footprint. Data center consolidation also supports DoD's cybersecurity initiatives by automating reporting and patch management. This consolidation will drive DoD down to a smaller physical footprint, but more importantly, it will place vital assets behind a sustainable layered defense. The below table summarizes DoD Data Center Consolidation Savings from fiscal year 2010 through fiscal year 2017. It is estimated that from fiscal year 2010 to the end of fiscal year 2016, DoD will have closed 944 data centers, saving a cumulative amount of $877M.

DOD Data Center Consolidation Savings Summary (FY10 - FY17)

Summary Metrics (1)(3)(5)	Prior Years (7)	FY 2014	FY 2015	FY 2016 (2)	FY 2017 (2)
Fiscal Year Data Center Closures	244	174	162	364	93
Fiscal Year Impacted Servers from Closures (4)	12,623	1,473	2,366	10,400	3,813
Fiscal Year Savings (6)		$34,034,475	$127,768,553	$566,058,687	$523,203,290
Cumulative Year Savings	$149,191,464	$183,225,939	$310,994,492	$877,053,179	$1,400,256,469

Notes:

(1) DOD Total Cost of Ownership Model Used (DOD DCC Model v 1.1_UNCLAS_FOUO_Final) for all datasets

(2) Forward looking projections. Both efficiency and facility consolidation savings estimated for FY16, FY17.

(3) In FY12 dollars

(4) Impacted Servers includes both decommissioned and moved servers.

(5) Investments required to implement efficiencies or close data centers are not captured within this analysis

(6) FY10 through FY12 savings are due to data center closures; not the achievement of efficiencies

(7) Prior Years equals the cumulative year savings between through FY13

D. Defend Against Cyber Attack

Cyber intrusions and attacks by both state and non-state actors have increased dramatically in recent years, putting DoD missions and information at risk. Adversaries continually adapt and evolve in response to cyber countermeasures, threatening DoD networks and systems. In March of 2015, Secretary Carter explained: “Cyberspace is presenting us with some of the most profound challenges, both from a security perspective and from an economic perspective … [and] our national leadership at every level is really seized with the need to get on top of this problem.” The next month, the DoD Cyber Strategy was released. Its purpose is to guide the development of DoD’s cyber forces, and strengthen cyber defense and cyber deterrence posture.

Nearly every single one of the successful network exploitations that DoD has had to deal with can be traced to one or more human errors on the network, which makes raising the level of individual awareness and performance in cybersecurity absolutely paramount. One of the areas in focus is a comprehensive review of how the Department is positioned to continue developing its cyberspace workforce, including skills mapping, roles and responsibilities, and required skills.

A holistic cybersecurity discipline culture is also critical to defending the Department’s information and information networks. DoD is working to transform its cybersecurity culture by improving human performance and accountability. DoD prioritized a list of key cyber efforts known as the Cybersecurity Discipline Implementation Plan. This is the roadmap to aggressively eliminating preventable cyber vulnerabilities that can put DoD missions at risks. Its implementation directly aligns to the DoD Cyber Strategy and to the DoD Cybersecurity Scorecard, which evaluates how DoD is doing on its path to reaching its goals in cybersecurity.
Priorities in the Cybersecurity Discipline Implementation Plan focus on four top Lines of Effort:

1. **Use Strong Authentication** – Eliminate the use of “replayable” authentication during log-on, such as usernames and passwords. Instead, move to a more secure two-factor authentication, utilizing cryptographic identity credentials issued by the DoD Public Key Infrastructure for everyone on DoD networks. This reduces the ability of adversaries to use stolen authenticators, and ensures that only legitimate credential holders are granted access. In turn, this degrades adversaries' ability to maneuver DoD networks.

2. **Harden All Devices** – Configure all DoD computers to the Department’s security standards; maintain secure configuration by patching aggressively. Establish protections to reduce spear phishing; diminish use of e-mail as a conduit for cyber-attackers to access DoD networks.

3. **Reduce the Attack Surface** – Ensure every Internet-accessible DoD website is housed in a demilitarized zone, separated from the larger DoD network. This limits the spread of successful attacks against these servers and helps cyber defenders focus their attention.

4. **Defend Every Computer** – Properly defend every DoD mission, as well as every computer and network device. Eliminate any gaps in coverage by DoD cyber defense organizations.

Using strong authentication, hardening all devices, reducing the attack surface, and defending every computer will diminish preventable cyber vulnerabilities that can put missions at risk, better defending the DoD’s information and information networks.

E. Empower Mobile Data Access

Mobility in the Department is evolving to meet the level of IT usage and consumerization set by commercial industry and expected by the DoD user base, while attempting to reduce costs. DoD began by consolidating the Department's IT infrastructure to support our existing mobile devices. Then, the Department adopted a multivendor approach, allowing the DoD Components to use the latest commercial devices that offer more capabilities – like mobile apps and GPS – to meet mission needs. These devices (and their apps) and are appropriately managed to meet DoD security requirements, but allow some flexibility for personal use capabilities, such as personal email or mobile apps for banking, news, and travel information. Moving forward, DoD will evaluate new mobile devices for approval, ensure the mobile infrastructure complies with DoD security policy, and adopt mobility focused business processes in an attempt to reduce cost.

The Department's mobile portfolio comprises of unclassified and classified mobile capabilities. In support of the DoD Mobile Unclassified Capability (DMUC), the foundational infrastructure has been built. It includes a mobile device manager and a mobile application store and Gateway for unclassified mobility that will leverage commercial carrier infrastructure and provide entry points for classified services. In the future, the DMUC infrastructure will evolve and become more global, enabling derived credentials at the end of 2015, wearables in 2016, and the Internet of Things in 2017. The DoD Mobile Classified Capability (DMCC) is transitioning from a previous capability based on Government Offered Solutions (GOTS) to a new DMCC based on commercial solutions. This is a significant change. DoD found that GOTS-based solutions were not user friendly, and only leveraged cellular 2G. In the future, DoD anticipates commercial solutions for classified with more capabilities, data-at-rest, apps and widgets, Top Secret / Secure Compartmentalized Information capability, and other approved devices.

The biggest challenge in mobility is security mobile devices while keeping up with the rapidly changing pace of mobile technologies. As a result, modernizing the Department's security approval process for mobile devices is one way in which DoD is empowering mobile data access for its users. In partnership with the National Security Agency (NSA), DoD is leveraging the National Information Assurance Partnership Common Criteria evaluation and validation scheme for mobility approvals. As of January 2016, Samsung and Boeing Black have validated Mobile Device Fundamentals Protection Profiled (PP) v2.0, and Apple and Windows have submitted PP v2.0 for unclassified mobile capabilities. Boeing Black has DMCC potential.

Mobile progress on the tactical edge illuminates the untapped potential of mobile capabilities for the Department. Tailored applications demonstrate the advantage of adapting mobility to military needs in areas such as training, with the Army Field Inspection Tool; operations, with the Air Force Electronic Flight Bag (EFB); tactical, with the Android Tactical Assault Kit (ATAK); and in training, with Combat Training Centers. EFB uses Apple iPads to replace heavy paper-based navigational charts and flight manuals, allowing flight crews to perform flight-management tasks more easily and efficiently. ATAK combines an Android device and tool suite connected to a tactical network/radio, providing users with up-to-the-second information about the environment around them. Capabilities provided to the warfighter include voice; text chat; video; images, an interactive, layered, shared, and moving map.

3. Last Year's Results (FY15 Budget Execution)

The DoD IT Budget is managed by aligning funds to capabilities beginning with four Mission Areas. These Mission Areas are:

- Enterprise Information Environment Mission Area (EIEMA)
- Business Mission Area (BMA)
- Warfighting Mission Area (WMA)
- Defense Intelligence Mission Area* (DIMA)

These Mission Areas are broken down into twenty-one segments or categories, the top six of which consumed a majority of the DoD IT budget in fiscal year 2015. Of the thousands of individual investments making up the entire unclassified portion of the DoD IT budget, nearly two-thirds of the investments were assigned to these six segments, making up more than 85% of the unclassified FY15 DoD IT budget (or 70% of the entire classified and unclassified IT Budget). These six segments are: DoD IT Infrastructure, Battlespace Networks, Command & Control, Logistics/Supply Chain Management, Human Resource Management, and Health. Mapping these six segments to mission areas, EIMA includes DoD IT Infrastructure (A); WMA includes Battlespace Networks (B) and Command & Control (C); and BMA includes Logistics/Supply Chain Management (D), Human Resources Management (E), and Health (F). Please note that DIMA consumed only 0.43% of the $38.2B budget. All of the segments categorized by mission area are represented in the table below:

Enterprise Information Environment	DoD IT Infrastructure
	IT Management
	Enterprise Services TBD
	Cyber Information & Identity Assurance
Business	Logistics/Supply Chain Management
	Human Resource Management
	Health
	Financial Management
	Acquisition
	Installation Support
	Business Services TBD
Warfighting	Command & Control
	Battlespace Networks
	Force Application
	Force Training
	Battlespace Awareness-Environment
	Protection
	Core Mission TBD
	Force Management
	Building Partnerships
Defense Intelligence	Battlespace Awareness-ISR

A brief discussion of most expensive investment from the execution of the fiscal year 2015 budget in each of the top six segments is provided below. These examples illustrate the spectrum of disparate programs and capabilities that – when consolidated and combined with the other investments in the DoD IT portfolio –enable and contribute to the fulfillment of the DoD's IT priorities.

A. DoD IT Infrastructure

Next Generation Enterprise Network Increment 1 (FY15: $1,058.2M; FY16: $1,337.9M)

Next Generation Enterprise Network (NGEN) is an enterprise network that will provide secure, net-centric data and services to Navy and Marine Corps personnel. It represents the continuous evolution of IT at the Department of Navy (DON). NGEN forms the foundation for the DON's future Naval Network Environment that will be interoperable with and leverage other DoD- provided Net-Centric Enterprise Services. NGEN directly supports the DoD IT priority of modernizing the networks – starting with JRSS – by procuring and installing a total of seven Installation Processing Nodes (IPNs) at seven different locations within and outside of the continental United States. This will provide better defense of DoD data and other resources against cyber threats through configuration management, engineering, integration and certification of hardware.

In FY15, NGEN financed the Technology Refresh Plan of fielded network equipment and components, completed procurement of the existing network infrastructure and cybersecurity, and completed the transition to the NGEN contract, including the Technology Refresh Plan. Funding also continued financing operations, including transport and enterprise services, end user services fees, cybersecurity, hardware usage fees, and procured software licenses to support more than 300,000 U.S. Navy users. Navy also consolidated four data centers into two with NMCI Data Center Consolidation Planning. Finally, Navy continued legacy network migration activities along with the engagement and alignment with emerging JIE architecture efforts.

In FY16, NGEN financed network infrastructure Tech Refresh, cybersecurity enhancements, various network consolidation initiatives, and software license procurement, as well as various modernization initiatives. Navy continued to finance operations, including transport and enterprise services, end user services fees, hardware usage fees, and software maintenance. Under the NGEN Mobility Strategy, Navy expanded mobile device capabilities, video, and mobile support for workflows. Finally, NGEN completed deployment of Traffic Engineering Tier 3 sites (41 sites), and continued the planning and execution for the NGEN Infrastructure Technology Refresh Strategy.

B. Battlespace Networks

Warfighter Information Network-Tactical Increment 2 (FY15: $421.1M; FY16: $501.2M)

Warfighter Information Network-Tactical (WIN-T) is the Army's Program to achieve a world-class Joint expeditionary network enabled by information technologies that support the goals of the Army Campaign Plan and other Army/Joint mandates. WIN-T is the cornerstone tactical communications system, the strategy for which is being implemented in the 2007 to 2027 timeframe. The WIN-T program is establishing a single integrating framework creating a network of networks for the Army, subject to commander's intent and security policy. WIN-T supports the DoD IT priority of empowering mobile data access by enabling the mobile warfighter to operate in a noncontiguous, or fragmented, battlefield environment.

In FY15, funds were used to field WIN-T for the following organizations:

- 3/82nd Air Assault (AA) Infantry Brigade Combat Team (BCT) at Ft Bragg
- 1st Armored Division (AD) Headquarters
- 1/1st AD Infantry BCT at Ft Bliss

- 3/2nd and 2/2nd Stryker BCTs at Joint Base Lewis-McChord4/10th Mountain Infantry BCT at Ft. Polk (reflagged as 3/10th)
- 2/101st Airborne (AB) and 3/101st AB Infantry BCT Engineering Company and Maneuver Battalion additions at Ft. Campbell
- 2/82nd AA Infantry BCT Engineering Company and Maneuver Battalion additions at Ft. Bragg
- 1st CAV Division Headquarters at Ft. Hood

The Program Office also completed the vehicle integration and training for the 25th Division Headquarters at Schofield Barracks.

FY15 funds were also used to deploy and integrate 101st AA Division HQ Tactical Communications Nodes (TCNs) into the AFRICOM overall mission support network as part of Operation United Assistance and the 82nd AA Division HQ, 2/82nd AA and 1/10th Mountain Infantry BCTs deployed in support of Operation Inherent Resolve.

During FY15, WIN-T Increment 2 successfully completed support to 2/1st AD Armor BCT and Network Integration Evaluation (NIE) 15.2 and 16.1. WIN-T Increment 2 participated as a baseline system in both events. The Program Office successfully completed Record Testing for the Joint Interoperability Certification (JIC) 2015 with 100% of the test threads completed with no issues. Certification was granted on January 15, 2016.

Additionally, the Army was authorized to enter into Full Rate Production (FRP) for the WIN-T Increment 2 program. The corresponding Acquisition Decision Memorandum (ADM) was signed on June 3, 2015. Similarly, the US Army Communications-Electronics Command (CECOM)granted WIN-T Increment 2 Full Materiel Release (FMR) based on satisfying conditions established by CECOM.

Finally, the DAE used FY15 funds to approve the WIN-T Increment 2 FRP Acquisition Program Baseline (APB). This APB provides updated program cost thresholds and establishes acquisition and sustainment affordability caps.

C. Command & Control

Air And Space Operations Center-Weapon System Increment 10.2 (FY15: $83.3M; FY16: $111.2M)

The Air Operations Center Weapon System (AOC WS) is the is the weapon system the Commander, Air Force Forces (COMAFFOR) provides the Combined/Joint Force Air Component Commander (C/JFACC) for planning, executing, and assessing theater-wide air and space operations. The C/JFACC provides air, space and cyber support to the combined/Joint Forces Commander (C/JFC) by coordinating, de-conflicting, and assessing the progress of various weapon systems to advance the C/JFC's campaign. The AOC WS develops operations strategy and planning documents. The weapon system also disseminates tasking orders; executes day-to-day peacetime and combat air, space, and cyber operations; and provides rapid reaction to immediate situations by exercising positive control of friendly forces.

The AOC WS Increment 10.2 program keeps the AOC interoperable, certified, supportable, and compliant through the integration, testing, and fielding of new capabilities and upgrades the AOC WS baseline. The program supports mission requirements at Geographic and Functional AOCs, as well as Support and Manpower Augmentation units. To keep the AOC current and interoperable with the Combatant Commands (CCMD), cyber requirements, and fifth generation weapon system/weapons, the AOC WS program plans to evolve the AOC through the integration and test of progressively improving capabilities. These activities ensure a system-of-systems engineering perspective for the AOC WS, and include weapon system standardization activities as defined by AOC WS requirements documents.

AOC Increment 10.2 received a Milestone B decision October 11, 2013. As a result of passing Milestone B, this program is in Budget Activity 5, System Development & Demonstration (SDD), It is conducting engineering and manufacturing development tasks aimed at meeting validated requirements prior to full fielding decision.

This project will provide for design, development, integration of third party capabilities, and testing; as well as, build-up and fielding, of the Help Desk (HD), Formal Training Unit (FTU), Combined Air Operations Center-experimental (CAOC-X) suite, and one geographic site.

Activities also include studies and analysis to support current program planning and execution, as well as future program planning, and transition to production and sustainment contract.

In FY15 AOC WS:

- Continued contractor modernization and provided contractor support for development and operational testing, training, and initial site deployment. This included but is not limited to obtaining an Interim Authority to Test (IATT).
- Prepared to obtain an Authority to Operate (ATO).
- Conducted the contractor System Acceptance Test (SAT).
- Conducted the Government Developmental Testing (DT) and the Operational Assessment.
- Conducted bill of Material (BOM) procurement pre-installation activities, site-preparations, and some on-site installation activities before the Initial Operational Test and Evaluation (IOT&E) sites began.

In FY16 AOC WS plans to:

- Complete contractor Design/Development
- Achieve Milestone C
- Provide contractor support for development and Operational Testing (OT) training and initial site deployment, including but not limited to the following:
  - Obtain an Authority to Operate (ATO)
  - Complete the Government Developmental Testing (DT) and Operational Assessment
  - Conduct initial Operational Test and Evaluation (IOT&E) activities, including:
    - Conduct of OT Phase I at the Combined AOC-Experimental (CAOC-X), focused on operational suitability
    - Fielding to the Formal Training Unit (FTU)

D. Logistics/Supply Chain Management

Global Combat Support System-Army Increment 1 (FY15: $244.9M; FY16: $288.7M)

Global Combat Support System (GCSS) – Army will provide Soldiers with a seamless flow of timely, accurate, accessible, actionable and secure information that is not readily available today. Empowering mobile data access will give combat forces a vital and decisive edge. GCSS-Army will modernize logistics by implementing best business practices to streamline supply operations, maintenance operations, property accountability, and logistics management and integration procedures in support of the Future Force transition path of the Army Campaign Plan.

In FY15, GCSS-Army:

- Continued fielding Wave 1 to the Army; fielding to an estimated 121 additional units by the end of FY15
- Completed Wave 2 development efforts as planned (Est. 3Q15)
- Completed fixes to errors found in the Operational Assessment of Wave 2
- Provided the Milestone Decision Authority an update prior to full fielding of Wave 2 to the Army
- Began fielding Wave 2 to the Army

In FY16, GCSS-Army will:

- Complete Wave 1 Fielding to the remaining units
- Continue fielding Wave 2 capability to the Army
- Continue Operation and Sustainment activities and Tier I/II/III Helpdesk, including software and hardware changes, fixes and improvements

E. Human Resource Management

Integrated Personnel And Pay System-Army Increment 2 (FY15: $79.8M; FY16: $140.5M)

Integrated Personnel and Pay System (IPPS) –Army Increment II will deliver fully integrated personnel and pay services for all Army Components that builds on the trusted database delivered by the IPPS-A Increment I program. Increment II will link the personnel and pay functions for all Army personnel, eliminating duplicate data entry, reducing complex system maintenance, and minimizing pay discrepancies. IPPS-A Increment II will account for status changes between Active, Reserve, and National Guard components, to ensure accurate service time and minimize impact on individual pay, credit for service, and other benefits, as well as enable disciplined human resource management. This will support DoD IT priority of managing DoD data.

FY15 funds were used to obtain a Milestone B Decision on December 19, 2014, and authority to award an Engineering, Manufacturing and Development contract for System Integration support. IPPS-A also began System Requirements Review (SRR). Major activities include Integrated Baseline Review (IBR), blueprinting of Authoritative Data Sources, preparation for DISA migration, Business Process Re-engineering (BPR), supporting MilPay transition, legacy system analysis with Functional Proponents, defining the development environment, developing PeopleSoft Training, and evaluating Risk Management Framework.

FY16 funds will complete the SRR, System Functional Review (SFR) and IBR with System Integrator. Preliminary Design Review for Increment II will also begin. All activities leading to IBR, Primary Design Review, and Critical Design Review (CDR) will be completed. Finally, configuration, development, integration, and testing activities for Release 2.0 will begin, and an Integrated Progress Review (IPR) with Milestone Decision Authority (MDA) for Releases 3.0 will be supported.

F. Health

Department Of Defense Healthcare Management System Modernization (FY15: $145.7M; FY16: $527.6M)

Plans for Electronic Health Record (EHR) modernization for the Defense Healthcare Management Systems Modernization (DHMSM) began in 2008. In 2011, the Program was expanded to include the Department of Veterans Affairs (VA) in a joint initiative to implement a new, integrated electronic health record for both DoD and the VA, called the Integrated Electronic Health Record (iEHR) program. Secretary of Defense guidance in 2013 mandated the following:

- DoD shall continue near-term coordinated efforts with VA to develop data federation, presentation, and interoperability. This near-term goal shall be pursued as a first priority, separately from the longer-term goal of health record IT modernization
- DoD shall pursue a full and open competition for a core set of capabilities for EHR modernization
- Modernization will acquire and support deployment, implementation, and sustainment of an EHR system that replaces the DoD legacy DMHS inpatient and outpatient EHR systems

Based on direction from the President, Congress, and Secretary of Defense, the USD (AT&L) signed several acquisition decision memorandums (ADMs) guiding DoD to establish three new program offices: Defense Healthcare Management Systems Modernization (DHMSM), which focuses on replacement of the existing electronic health record systems; Defense Medical Information Exchange (DMIX), which focuses on the data-sharing efforts with DoD, VA, and private sector partners; and Joint Operational Medical Information System (JOMIS), which comprises the Theater Medical Information Program – Joint (TMIP-J) program and elements of the Medical Communications for Combat Casualty Care (MC4) program office. DMIX had three existing initiatives transferred to the program office (1) Virtual Lifetime Electronic Record-Health (VLER–Health), (2) James A Lovell Federal Health Care Center (JAL FHCC), and (3) existing data sharing efforts managed under the Defense Health Agency Health IT Directorate. The remaining iEHR Increment 1 (iEHR Inc 1) was significantly de-scoped to only the Medical Single Sign-on/Context management (MSSO/CM) implemented at James A. Lovell Federal Health Care Center (JAL FHCC), and is sustained as part of the JAL FHCC effort. These program offices are under the direction of the Program Executive Office Defense Healthcare Military Systems.

Selected FY15 accomplishments include but are not limited to:

- Completed the following Acquisition Documentation to support Authority to Proceed (ATP) for Contract Award.
    - Acquisition documentation completed includes:
        - Acquisition Strategy
        - Business Case
        - Engineering Master Plan
        - Cost and Benefit Analysis
        - Test Strategy
        - Deployment and Training Change Management Plan (DTCM)
        - Life Cycle Supportability Plan [LCSP])
    - The DHMSM Program Office received approximately 1,300 comments.
    - The Program Office favorably adjudicated to ensure that each and every comment received in reference to the acquisition documents was given the proper consideration in reaching an agreed upon resolution
    - As a result, the Program Office delivered quality acquisition documents that were thoroughly vetted and reviewed internally and by external organizations.

- Achieved Authority to Proceed (ATP) for contract award was achieved. This was preceded by several steps, such as:

  - IOC Site Readiness Report, to include preparation activities, change management, training, deployment, and testing to indicate the sites are ready for Contractor interaction
  - Reconciliation Report of functional workflow analysis, led by clinical champions, indicating alignment of capabilities with operations
  - Report indicating GAL readiness and ability to proceed with testing
  - Funding confirmation to prepare and process individual task orders
  - Updated Acquisition Documents as required

  Selected FY16 plans include but are not limited to:

- Initial Design Review/Final Requirements Review
- Formal (or Final) Design Review/Test Readiness Review
- System Verification Review/Operational Test Readiness Review
- Configuration & Integration Test
- Developmental Test & Evaluation
- Training for Subject Matter Experts
- Limited Fielding Training
- Installed at Initial Operational Capability Sites
- Continue Configuration and Integration of solution in testing environment
- Continue Independent Verification and Validation (IV&V)

4. Next Year's Objectives (FY17 Budget Request)

The DoD IT Budget is managed by aligning funds to capabilities beginning with four Mission Areas: EIMA, WMA, BMA, and DIMA. These Mission Areas are broken down into twenty-one segments or categories, the top six of which consumed a majority of the DoD IT budget in fiscal year 2015. These segments are: DoD IT Infrastructure, Battlespace Networks, Command & Control, Logistics/Supply Chain Management, Human Resource Management, and Health. (*Please reference the introduction to section #3 for additional information about these mission areas and categories.*)

A brief discussion of the five most expensive investments from the fiscal year 2017 budget request in each of these top six segments is provided below. These examples illustrate the spectrum of disparate programs and capabilities that – when consolidated and combined with the other investments in the DoD IT portfolio –enable and contribute to the fulfillment of the DoD's IT priorities.

A. DoD IT Infrastructure

Top 5 Investments within Segment	*FY17 ($M)*
Next Generation Enterprise Network Increment 1	*$1,272*
Defense Information System Network	*$867*
Network Enterprise Technology Command	*$634*
Non-DISN Telecomm	*$558*
Commercial Satellite Communications	*$511*

Next Generation Enterprise Network Increment 1 (FY17 $1,272M)

Next Generation Enterprise Network (NGEN) is an enterprise network that will provide secure, net-centric data and services to Navy and Marine Corps personnel and represents the continuous evolution of information technology at the Department of Navy. NGEN forms the foundation for the DON's future Naval Network Environment that will be interoperable with and leverage other DoD-provided Net-Centric Enterprise Services. NGEN directly supports the DoD IT priority of modernizing the networks – starting with JRSS – by procuring and installing a total of seven Installation Processing Nodes (IPNs) at seven different locations within and outside of the continental United States. This will provide better defense of DoD's data and other resources against cyber threats through configuration management, engineering, integration and certification of hardware.

In FY17, funds will be used to:

- Provide manpower for network command, control, and operations, provide seat services for Navy Working Capital fund activities
- Fund the enterprise operation for the NGEN network, including the enterprise fixed costs, award fee, software assurance (maintenance) for core build software application, various circuits, and program office support, as well as for Technical Refresh (TR) and Operation Rolling Tide (ORT)

Defense Information System Network (FY17 $867M)

The Defense Information System Network (DISN) is DoD's consolidated worldwide telecommunications infrastructure that provides end-to-end information transport for DoD operations, providing Combatant Commanders (COCOMs), Military Departments, Defense Agencies, the Warfighter, and our Mission Allies with a robust Command, Control, Communications, Computers and Intelligence (C4I) information long-haul transport infrastructure.

As a Mixed Life Cycle Program, DISN's primary focus is sustainment of the existing network. Transport provides a robust worldwide capability to transmit voice, video, data, and message traffic. DISA must provision, install, and maintain the network to support those capabilities. Real Time Services provide precedence-based assured services for voice and video over converged IP End-to-End. Voice reflects the consolidation of secure and unsecured voice services, while Video provides global, interoperable unclassified and classified video services with full-service video teleconferencing. DISN Internet Protocol (IP) services are the Secret IP Router Network and unclassified but sensitive IP Router Network. Joint World-wide Intelligence Communications System (JWICS) provides voice, video, and data communications and collaboration in support of the President, the Secretary of Defense, the National Intelligence Community, and DoD. The Operational Support Services (OSS) was created to manage the Telecommunications Management Network and tools that automate DISN's operation, administration, maintenance and provisioning functions while promoting efficiencies through consolidation, automation, and standardized data sharing. Acquisition fills any requirement deficiencies through a continuous infrastructure modernization to transition to IP capabilities by replacing or refreshing the optical core to 100G.

FY17 funds will be used to:

- Continue to enhance current Test and Evaluation (T&E) capabilities by employing automation technologies making these capabilities accessible to customers via the cloud in a self-service mode
- Employ new technology and methodology to conduct data analysis in the operational environment promoting continuous assessment of capability performance
- Implement automation of T&E services through the use of virtualization and cloud technologies thus reducing contractor support for these services and the reduction of contractor support for Tactical Edge Testbed and methodology development
- Continue to enhance OT&E processes, procedures, and tools through the use of automation and virtualization to improve operational testing capabilities for evolving requirements to better evaluate performance
- Analyze/prototype cloud computing services and open source capabilities for integration and interoperability with DoD capabilities

Network Enterprise Technology Command (FY17 $634M)

Network Enterprise Technology Command (NETCOM)/9th ASC became a direct reporting unit (DRU) assigned to the Army Chief Information Officer (CIO/G6) on Oct. 1, 2002. NETCOM/9th ASC became the operational executive agent for Army-wide network operations and security: the single point of contact for Army network development and protection, offering seamless C4 information management of common-user services in support of the combatant commanders and Army service component commanders. As such, the mission of NETCOM/9th ASC entailed the provision of technical control and support for Director of Information Management operations; the operation and management of the Army's total information infrastructure; and the management and defense of the Army frequency spectrum.

FY17 funds will be used to support the U.S. Army Network Enterprise Technology Command which plans, engineers, installs, integrates, protects, defends and operates Army Cyberspace, enabling Mission Command through all phases of Joint, Interagency, Intergovernmental and Multinational operations.

Non-DISN Telecommunications (FY17 $558M)

This investment reflects non-DISA managed telecommunications costs previously reported under the DISN line. The DISA Transformation initiative identified the need to properly display these costs. The costs reflect telecommunications costs for the Federal Technology Service (FTS) and other telecommunications support where DISA provides contracting services but does not manage the costs.

FY17 funds will be used to manage the costs for the Federal Technology Service (FTS) and other telecommunications support where DISA provides contracting services, but does not manage the costs.

Commercial Satellite Communications (FY17 $511M)

This investment delivers Commercial Satellite communications (COMSATCOM) services, to remain a value added service through fostering increased competition/competitive pricing for COSMATCOM services and expanding service offering as well as to continuously educate the customer base on currently available COMSATCOM capabilities and product offerings, enabling the best-possible decision making by DoD leadership for mission success.

FY17 funds will be used to budget for the COMSATCOM Center, which acts as an interface between the customer, the contracting organization, and the commercial satellite service providers. Requirements for Fixed Satellite Service (FSS), Mobile Satellite Service (MSS), and Enhanced Mobile Satellite Service (EMSS) are funded by customers via the Defense Working Capital Fund (DWCF). The Life Cycle Management provided by COMSATCOM Center is funded by a surcharge when customers order services, such as:

- Space segment resources such as full or partial transponder leases
- Antenna, terminal, and teleport services
- Managed services such as dynamically assigned bandwidth or Internet Protocol (IP) over SATCOM
- Host Nation Approval (HNA)
- End-to-end turnkey solutions
- Special features such as portability or bandwidth management
- Expedited services for critical circumstances
- Airtime
- Equipment

B. Battlespace Networks

Top 5 Investments within Segment	*FY17 ($M)*
Warfighter Information Network-Tactical Increment 2	*$394*
Consolidated Afloat Networks And Enterprise Services	*$315*
Joint Tactical Radio System Handheld, Manpack, And Small Form Fit Radios	*$307*
White House Communications Agency	*$187*
Joint Battle Command-Platform	*$143*

Warfighter Information Network-Tactical Increment 2 (FY17 $394M)

Warfighter Information Network-Tactical (WIN-T) is the Army's Program to achieve a world-class Joint expeditionary network enabled by information technologies that support the goals of the Army Campaign Plan and other Army/Joint mandates. WIN-T is the cornerstone tactical communications system, the strategy for which is being implemented in the 2007 to 2027 timeframe. The WIN-T program is establishing a single integrating framework creating a network

of networks for the Army, subject to the Commander's intent and security policy. WIN-T supports the DoD IT priority of empowering mobile data access by enabling the mobile warfighter to operate in a noncontiguous, or fragmented, battlefield environment.

In FY17, funds will be used to support the maturation of the SATCOM On-The-Move (OTM) antenna (delivered by Distributed Embedded SATCOM OTM Standard Terminal Architecture (DESSTA)), procure Lot 7 Configuration Items (CIs) for 2 Infantry Brigade Combat Teams (IBCTs) and to field to five IBCTs, one Division, six IBCT Engineering Companies and Maneuver Battalions, and one SBCT Engineering Company.

Consolidated Afloat Networks and Enterprise Services (FY17 $315M)

Consolidated Afloat Networks and Enterprise Services (CANES) is the Navy's only Program of Record (POR) to replace existing afloat networks and provide the necessary infrastructure for applications, systems, and services to operate in the tactical domain. CANES is the technical and infrastructure consolidation of existing, separately managed legacy afloat networks currently under Ship Communications Automation. The legacy, afloat network designs are at their End of Life. CANES will provide complete infrastructure – including hardware, software, processing, storage, and end user devices – for Unclassified-Sensitive Compartmentalized Information, for all basic network services, such as email, web, chat, and collaboration, to a wide variety of Navy surface combatants, submarines, Maritime Operations Centers, and Aircraft. Approximately 36 hosted applications and systems, including Command and Control; Intelligence, Surveillance, and Reconnaissance; Information Operations; Logistics; and Business domains require the CANES infrastructure to operate in the tactical environment. Specific programs – such as Distributed Common Ground System - Navy (DCGS-N), Global Command and Control System - Maritime (GCCS-M), Naval Tactical Command Support System (NTCSS), and Undersea Warfare Decision Support System (USW-DSS) – depend on the CANES Common Computing Environment to field, host, and sustain their capability because they no longer provide their own hardware. CANES requires Automated Digital Network System to field prior to or concurrently with CANES due to architectural reliance between the two programs.

FY17 funds will be used to continue the replacement of legacy network designs using the following appropriations:

- MILPERS – Funds are used for program management of the CANES acquisition program
- DWCF – Funds the network and communications infrastructure aboard Military Sealift Command ships that are equipped with the Navy's standard solution
- Operations – Funds are used to sustain CANES and Legacy network systems, including program management, In-Service Agent (ISEA) support, and annual software license fees
- Procurement – Funds are for the procurement of (9) Afloat production units, (4) Afloat Technical Insertion units, (1) Afloat First Article, and (1) Ashore production unit, with integration, and associated costs for pre-installation design. In addition, the FY17 CANES investment will fund installation of (21) Afloat production units and (1) Ashore production unit.
- Research, Development, Text & Evaluation (RDT&E) – CANES will support developmental efforts for Technical Insertion (TI) software baseline, perform systems engineering efforts to complete functional baselines and updates to technical data packages, continue testing events at Enterprise Engineering and Certification (E2C) laboratory for TI software baseline, perform Developmental Testing (DT) and Follow-On Test and Evaluation (FOT&E) for force level platforms, and perform development for CANES objective platforms

Joint Tactical Radio System Handheld, Manpack, And Small Form Fit Radios (FY17 $307M)

The Joint Tactical Radio System Handheld, Manpack, and Small Form Fit Radios (JTRS HMS) program is an Acquisition Category (ACAT) 1D program developing the materiel solution to provide Software Communications Architecture (SCA) compliant radios to Warfighters. The program meets the radio

requirements for Soldiers and small platforms, such as missiles and ground sensors. JTRS HMS Increment 1 is structured as a single Program of Record (POR) with two phases.

- Phase 1 developed Small Form Fit (SFF) SFF-A (1 and 2 Channel), SFF-D and AN/PRC-154 Rifleman Radio for use in a sensitive but unclassified environment
- Phase 2 will develop the 2 Channel Manpack (MP) and SFF-B for use in a classified environment

JTRS HMS radios are designed to host SCA compliant software waveforms and applications. Phase 1 radios will host the Soldier Radio Waveform (SRW). Phase 2 will host the SRW, Ultra High Frequency (UHF) Satellite Communications Military, Single Channel Ground to Air Radio System (SINCGARS), and Mobile User Objective System (MUOS) waveforms. JTRS HMS will provide new networking capability to the individual Soldiers, Marines, Sailors, and Airmen and also continue to provide legacy radio interoperability. JTRS HMS will support the Net Centric Transport goal of traffic convergence on a single Internet Protocol (IP) internetwork by running JTRS networking services with the SRW.

JTRS HMS provides the Warfighter with a software reprogrammable, networkable multi-mode system (of systems) capable of simultaneous voice, data, and video communications. The program encompasses specific requirements to support the US Army, US Navy, US Marine Corps, US Air Force and the Special Operations Command (SOCOM) communication needs.

FY17 funds will procure modified non-developmental items (NDI) through two full and open competition contracts open to all potential industry partners. The contracts will procure NDI Rifleman Radios (RR) and Manpack (MP) Radios for use in a classified environment. The Army will award Multiple Firm Fixed-Price (FFP) Contracts through a multiple step selection process:

- Award FFP Contracts and initial delivery orders to all qualified vendors based on technical acceptability and demonstrations (RR Awarded 29 April 2015 and 3QFY16 for MP).
- Award FRP delivery orders based on operational tests and best value trade off construct (1QFY17 for RR and 3QFY18 for MP).

By Procurement funding will be utilized for:

- Manpack Full Rate Production Award – To Purchase a small lot of Manpack Radios from all qualified vendors on the Full Rate Production Contract for to complete an Operational Test in support of final Full Rate Production Award
- Integration of the Radios into Vehicles and the associated Non Recurring Engineering, such as plans and schematics

By RDTE funding will be utilized for:

- Manpack Qualification Test – To test vendors previously purchased radios to ensure they meet the minimum requirements laid out in the Full Rate Production Contract
- Complete Rifleman Radio Operational Test – To determine which radios will be purchased for Full Rate Production going forward
- Provide technical and engineering support for development efforts including preparing for Full Rate Production for Rifleman and Manpack Radios
- Perform Government Development Test, including the participation in the Navy Mobile User Objective System (MUOS) End to End Demonstration and Multiservice Operational Test & Evaluation with MUOS waveform on the Manpack

White House Communications Agency (FY17 $187M)

The White House Communications Agency (WHCA) is a joint service military agency under the operational control of the White House Military Office (WHMO) and administrative control of the Defense Information System Agency (DISA). The mission of WHCA is to provide telecommunications and other related support to the President of the United States (POTUS) in his role as Commander in Chief (CINC), Chief Executive Officer of the United States, Head of State, and other elements related to the President. Elements related to the President include the Vice President, the First Lady, the first family, the United States Secret Service (USSS), the White House Staff, the White House Press Office, the National Security Staff, WHMO, and others as directed.

Although WHCA provides a wide variety of services, the core of the agency's mission is to provide instantaneous secure and non-secure voice and five minute record communications support to the POTUS anytime, anywhere. Other voice, video, and data communications services are provided as necessary to allow for staff support and protection of the POTUS. WHCA also provides the POTUS and Vice President (VPOTUS) audiovisual and photographic services on a reimbursable basis, including but not limited to: video tape recording for the President and others as directed, photographic laboratory and graphics support to the White House, and general purpose automated data processing support for the National Security Staff (NSS) and the White House. This support is provided in Washington DC and at trip sites worldwide. To support this requirement, WHCA's organization is structured to allow for Fixed and Deployable (Travel) support.

In FY17, two appropriations will support:

- Operations & Maintenance: The WHCA is a joint service military agency under the operational control of the White House Military Office (WHMO) and administrative control of the Defense Information Systems Agency (DISA). WHCA’s mission is to provide information services to the POTUS, VPOTUS, National Security Council, USSS, and others as directed by WHMO ensuring the ability to communicate anywhere, anytime, by any means to anyone in the world, in accordance with Public Law 109-163. This support is provided in Washington, DC, at worldwide travel sites, and in second residences. Information services are also provided to the Presidential Information Technology Community. To meet its requirements, WHCA is structured to allow for fixed and travel (deployable) information services.

- Procurement: WHCA's Presidential Communications Vision 2020 (PCV 2020) is the central theme of WHCA's Strategic Plan and approach for transformational modernization and innovation to ensure POTUS/VPOTUS can communicate anywhere, anytime, by any means with anyone in the world. PCV 2020 is WHCA's means to achieve four segment architectures critical to WHCA's mission providing world class mobile Presidential Communication Services. This vision incorporates DoD modernization tenets for Senior National Leadership communications, Command and Control, Mobility, Cybersecurity, and the Joint Information Environment: the WHMO Mobility Vision (Mobile, Virtual Network Enterprise), POTUS Wireless Ecosystem (fully enabled ubiquitous network mobile and wireless Tripsite), Strategic Support Environment (PCI Information Environment), and Voice and Video Call Center (Virtual community gateway supporting enterprise collaboration, social media, virtual events, and networking capabilities for personnel supporting Presidential events).

Joint Battle Command-Platform (FY17 $143M)

Joint Battle Command-Platform (JBC-P) is a foundation for achieving information interoperability between joint warfighting elements on current and future battlefields. As the follow on program to Force XXI Battle Command Brigade & Below (FBCB2) technology, it will be the principal command and control system for the Army and Marine Corps at the brigade and below level, providing users access to the tactical information necessary to achieve information dominance over the enemy. It consists of computer hardware and software integrated into tactical vehicles, aircraft, and provided to dismounted forces. JBC-P uses a product line approach to software development to save cost and promote a common architecture. Components include a core software module that provides common functionality required of all platforms and tailored software modules with unique capabilities for dismounted, vehicle, logistic, aviation, and command post elements. JBC-P software is designed for use over the Blue Force Tracking II transceiver and associated satellite networks, as well as ground-

based networks. Other key enhancements include a redesigned, intuitive user interface and faster mapping software to quickly process and display critical graphics. It will be the primary provider and user of digital battle command and situational awareness across the spectrum of operations and will allow warfighters to more effectively and consistently communicate critical information over networks that connect the most distant and remote locations.

JBC-P software is designed to run on existing FBCB2 systems as well as new hardware items, reducing the Army's investment in new hardware. In addition to utilizing the FBCB2 systems, JBC-P provides new hardware capabilities including Dismountable Vehicle Computer Systems, one way beacons, and ancillary equipment, such as Type 1 Encryption Device, Mission Data Loader, Disc Duplicator, cables, and installation kits.

FY17 funds will enable the procurement of vehicle platform computer systems, 300 Command Post systems, Satellite Transceivers, Encryption Devices, ancillary equipment, training, fielding, publications and support equipment.

C. Command & Control

Top 5 Investments within Segment	*FY17 ($M)*
Air And Space Operations Center-Weapon System Increment 10.2	*$434*
Next Generation Operational Control System	*$332*
AF NC3-MEECN Modernization	*$279*
Tactical Mission Command	*$157*
Global Command And Control System- Joint	*$150*

Air And Space Operations Center-Weapon System Increment 10.2 (FY17 $434M)

The Air and Space Operations Center-Weapon System (AOC WS) is the primary air, space, and information operations C2 (Command and Control) capability that the Joint Force Air Component Commander provides to the Commanders of Unified Combatant Commands. The AOC WS consists of several nodes that together provide a full range of global C2 capabilities. Some AOCs are located within regional Area of Responsibility to provide C2 support to their respective Combatant Commander's (COCOMs). Others support global operations, such as Air Force Global Strike Command and Air Force Space Command. Under Title 10 authority, the Department of the Air Force is responsible for organizing, training, equipping and providing forces to the Unified Combatant Commands in support of Air and Space operations within the COCOM.

In FY17, funds will be used conduct the initial installation of AOC WS Increment 10.2 on four geographic nodes as well as support for continued technical refresh on the 10.2 system. Additionally, funds will begin to sustain the Increment 10.2 baseline post Full Deployment Decision. This will support the DoD IT priorities of modernizing the networks and sharing with mission partners.

Next Generation Operational Control System (FY17 $332M)

The Global Positioning System (GPS) Next Generation Operational Control System (OCX) program procures and fields a modernized satellite command and control (C2) system capable of operating all GPS III and legacy satellites. This includes telemetry tracking control and disposal operations for the primary and secondary payloads. OCX will also provide the operational capability for all new modernization features such as SAASM, M-Code and Flex-power while maintaining the ability to monitor and control existing legacy GPS signals. The new system will include increased information assurance protection and computer security over the existing GPS Architecture Evolution Plan. Acquisition of the new OCX system will be delivered in various blocks, to support the delivery of new GPS III capabilities.

FY17 funds will be used for OCX Development the GPS next generation operational control system to launch and operate GPS II and GPS III constellation and provide a robust Information Assurance system. Funds will also enable Air Force to certify and accept OCX Block 0 for launch and checkout operations of GPS-III satellites as well as develop command and control for GPS II satellites, legacy signals, and the modernized aviation safety of life signal (L5). Additionally, funds will enable the Air Force to continue the development of OCX Block 1 and Block 2 including remaining civil and military modernized signals (L1C and M-code). With regards to technical support, FY17 funds will provide the development of the Standardized Space Trainer (SST) to provide GPS III operator training and conduct and automation study to examine the feasibility of implementing control segment automation to increase command and control efficiencies. Facilities upgrades for Control Stations and associated equipment and servers.

AF Nuclear Command, Control & Communications – Minimum Essential Emergency Communications Modernization (FY17 $279M)

AF Nuclear Command, Control & Communications (NC3) systems provide assured communications between the President and strategic forces in nuclear environments. NC3 systems support the nuclear community with the following capabilities:

- Enabling assured Command and Control (C2) of Force Application
- Providing Force Direction
- Providing hardened communications for Emergency Action Message (EAM) delivery
- Providing AF Minimum Essential Emergency Communications (MEECN) capabilities
- Supporting Weapon System C2 communication

FY17 funds will be used for the Minuteman MEECN (Minimum Essential Emergency Communications) program to continue installation into Minuteman Intercontinental Ballistic Missile (ICBM) Launch Control Centers FY17 to replace the Minuteman MEECN Program (MMP). Funds will also enhance the Global Aircrew Strategic Network Terminal (Global ASNT), which anticipates obtaining milestone C decision FY17 and which will begin the production and development phase, nearing a solution to modernize and replace the Single Channel Anti-jam Man-Portable (SCAMP).

Tactical Mission Command (FY17 $157M)

Tactical Mission Command/Maneuver Control System (TMC/MCS) is a suite of products that provide Army and Joint community commanders and their staff with a human-centered collaborative capability, including integrated Voice over Internet Protocol (VoIP), a user-defined common operational picture (COP), and real-time situational awareness. TMC supports Army Battle Command System interoperability, as well as coalition interoperability to support Battle Staff functions. In addition, TMC funding provides a tactical SharePoint portal, aids in data management, and offers enterprise services, such as e-mail, Active Directory, security, data backup, and failover capabilities. TMC as defined by the elements below represents the evolution of the program.

FY17 funds will allow the Army to:

- Complete development, integration, certification, and operational testing of the Army COE version 2 baseline, and begin fielding that baseline in accordance with HQDA fielding directives.
- Continue to field and support the Army COE version 1 baseline in accordance with HQDA fielding directives
- Migrate the Command Post of the Future (CPOF) thick client workstation to sustainment, allowing all program resources to be focused and prioritized to COE directives and implementations
- Begin supporting the design and engineering of the Army COE version 3 baseline in coordination and cooperation with the community of PORs that comprise the Army Command Post Computing Environment (CP CE)

Global Command And Control System- Joint (FY17 $150M)

The Global Command and Control System-Joint (GCCS-J) Program Element funds a Joint Command and Control (JC2) portfolio that includes GCCS-J, Joint Planning & Execution Services (JPES) and supports the development and sustainment of the JC2 Architecture. GCCS-J is a suite of mission applications/systems that provide critical joint warfighting C2 capabilities by presenting an integrated, near real-time picture of the battlespace for planning and execution of joint military and multinational operations. GCCS-J, the Joint C2 System of Record, currently consists of three primary baselines: the Joint Operations Planning & Execution System (JOPES) and GCCS-J Global, which contains Integrated Imagery and Intelligence (I3), Situational Awareness/Common Operating Picture (COP) capabilities, and supporting infrastructure. The Status of Resources & Training System (SORTS) transferred programmatic responsibility from GCCS-J to OSD P&R at the end of FY11.

The GCCS-J program, at large is responsible for sustaining current operational baselines, modernizing key capability areas, and synchronizing across the Family of Systems (FOS). GCCS-J is used by all nine combatant commands (COCOMs) at sites around the world, supporting joint and coalition operations. Additionally, through the continued evolution of the GCCS Family of Systems (FoS), the Services also utilize components of the GCCS-J infrastructure to build their Service-unique variants, reducing the number of unique components as a result. JPES produces enhancements to the Joint Operations Planning and Execution System (JOPES), focuses adaptive planning capabilities, and provides a set of core infrastructure services necessary to provide the warfighter an interoperable environment where functionality can be easily added as mission needs dictate. The Joint C2 Architecture is a reference architecture that aligns to the DoD Information Enterprise Architecture (DoD IEA). It describes architectural concepts and technical constructs, and contains reference information related to the physical, software, information assurance, and data standards applicable to joint C2 capabilities integration and interoperability. It is designated an authoritative source of information and technical direction for the joint C2 capability area to enable capability investment and modernization planning in support of Department objectives and minimize integration risks as capabilities are developed and deployed. FY17 funds will enable DISA to:

- Provide critical operational fixes and Information Assurance & Vulnerability Assessment (IAVA) patches
- Sustain GCCS-J modernization initiatives
- Continue to terminate obsolete capabilities as modernization initiatives become operational
- Synchronize between FoS and GCCS-J efforts on client consolidation activities to replace or transition existing Global clients in alignment with user and FoS priorities/requirements
- Continue Human Factors Engineering (HFE) analysis and development with community to revamp look and feel of joint C2 apps/capabilities
- Develop additional plug-ins to satisfy new/emergent COCOM and Service requirements , coordinate on availability of functionality to FoS
- Sustain operational frameworks and associated plug-ins/widgets, such as help desk support and license maintenance
- Continue modernization efforts targeted at priority sustainment cost drivers: client consolidation
- Continue adaptive planning enhancements
- Continue improvements to/expansion of JFW services, including replacement for newsgroups, workflow Management service, administration services for monitoring, and management of austere environments
- Thoroughly test, harden, and scale JFW to meet the operational needs of all the systems

D. Logistics/Supply Chain Management

Top 5 Investments within Segment	*FY17 ($M)*
Global Combat Support System-Army Increment 1	*$284*
Logistics Modernization Program Increment 1	*$138*

DLA Enterprise Business System	*$110*
Navy Enterprise Resource Planning	*$99*
Global Combat Support System-Marine Corps Logistics Chain Management Increment 1	*$79*

Global Combat Support System-Army Increment 1 (FY17 $284M)

Global Combat Support System (GCSS) – Army will provide Soldiers with a seamless flow of timely, accurate, accessible, actionable and secure information that is not readily available today. Empowering mobile data access will give combat forces a vital and decisive edge. GCSS-Army will modernize logistics by implementing best business practices to streamline supply operations, maintenance operations, property accountability, and logistics management and integration procedures in support of the Future Force transition path of the Army Campaign Plan.

FY17 funding will continue sustainment operations of GCSS-Army Increment I solution - including help desk, software maintenance, and production support. GCSS-Army sustainment activities will increase through deployment until scheduled completion in FY17. In FY17, funds will also be used to support the full fielding of GCSS-Army Wave 2 functionality to remaining users; finalize Wave 2 development of the Property Book, Maintenance, Supply and Finance Solution; and complete large break fixes during and after full deployment.

Logistics Modernization Program (LMP) Increment 1 (FY17 $138M)

Logistics Modernization Program (LMP) delivers a fully integrated suite of software and business processes, providing streamlined data on maintenance, repair, and overhaul, planning, finance, acquisition, weapon systems supplies, spare parts, services, and materiel. As the Army's core logistics IT initiative, LMP replaced the two largest Army Materiel Command (AMC) National-level logistics systems: the inventory management Commodity Command Standard System (CCSS), and the depot and arsenal operations Standard Depot System (SDS). LMP meets the Army IT logistics vision of an overdue transformation from legacy National level applications to a modernized logistics enterprise solution across AMC to arsenals, depots, and other non-depot maintenance activities at the National level and the Defense Finance Accounting Service (DFAS). LMP support will allow the Army to achieve an integrated enterprise solution that enables materiel readiness and provides asset management and accountability, architecture, and acquisition compliancy and financial transparency.

LMP Increment 1 manages approximately 2 million transactions daily, valued at approximately $22 billion in inventory, and interfaces with more than 70 DoD systems, to include interfaces with other Army Enterprise Resource Planning (ERP) systems currently under development - Army Enterprise Systems Integration Program (AESIP), Global Combat Support System-Army (GCSS-Army), and General Fund Enterprise Business System (GFEBS). LMP Increment 1 was fully fielded in October 2010, and is currently used by approximately 21,000 users at more than 50 Army and DoD Continental United States (CONUS) and Outside the Continental United States (OCONUS) locations, including the Army's Communications-Electronics Command (CECOM) Life Cycle Management Command (LCMC), Aviation and Missile Command (AMCOM) LCMC, Tank-Automotive and Armaments Command (TACOM) LCMC, Joint Munitions and Lethality (JM&L), Army Sustainment Command (ASC), and all depots and arsenals in the Industrial Operations Activity Group, as well as DFAS.

FY17 funds will allow the Army to implement or execute the:

- Compliance / Auditability release, to include testing and release to Production (Oct 16)
- Major functional release to include completion of development, testing and release to Production
- Completion of corrective, preventative, and adaptive maintenance for deployed operational baseline as prioritized by AMC
- Transition of remaining seven sustainment service areas planned
- Retirement or transition of residual legacy systems to complete
- DISA Migration activities
- Continuation of decommission activities for the Secondary and Primary LMP Data Centers
- Software and the LMP Help Desk managed by ALTESS

Defense Logistics Agency Enterprise Business System (FY17 $110M)

Enterprise Business System (EBS) is a robust Commercial-Off-The-Shelf (COTS)-based ERP enterprise system which is secure, flexible, integrated, and inter-connected. Its primary mission is financial reporting, supply chain management, and logistics support; it is DLA's core financial system. The DLA EBS uses COTS products to provide an Enterprise Resource Planning (ERP) solution approach to manage all of DLA's supply chains. DLA introduced its first complete ERP solution through the Business Systems Modernization (BSM) Program, which was fully operational in 2007. BSM and other complementary systems now comprise the Enterprise Business System (EBS).

In support of the DLA Strategic Plan, the FY17 planned investment objectives include the continuous modernization and refinement of EBS through process and technical improvements by leveraging technology and area business reengineering opportunities. DLA will proactively look to leverage best practices and maximize the ability to rapidly deploy new technology. DLA continuously assesses EBS to determine the required modifications necessary for Process Excellence (PE) and to identify and implement priority mission essential changes. These modifications are captured as enhancements to EBS functionality.

Navy Enterprise Resource Planning (FY17 $99M)

The Navy Enterprise Resource Planning (Navy ERP) Program was established to transform and standardize Navy business processes for key acquisition, financial, and logistics operations. Navy ERP combines business process reengineering (BPR) and industry best practices, supported by commercial off-the-shelf software, and integrates all facets of a business, using a single database to manage shared common data. Navy ERP will be a major component of the Navy's Global Combat Support System family of systems and will provide a critical link between operating forces and support activities. Navy ERP will: reduce the Navy's overall costs by applying proven industry best practices and processes and replacing legacy IT systems; facilitating an end-to-end supply chain solution; integrating financial management, workforce management, inventory management, and material operations; and, enabling rapid response to operating force logistics needs.

Navy's FY17 funds will:

- Operate & maintain 24/7 availability of the Navy ERP Production System, such as data and disaster recovery center operations as well as hardware and software license maintenance
- Provide on-going end user and Help Desk services for about 72,000 users at organizations including:
  - Naval Air Systems Command (NAVAIR)
  - Naval Supply Systems Command (NAVSUP)
  - Space and Naval Warfare Systems Command (SPAWAR)
  - Naval Sea Systems Command (NAVSEA)
  - Office of Naval Research (ONR)
  - Strategic Systems Programs (SSP)

Global Combat Support System-Marine Corps Logistics Chain Management Increment 1 (FY17 $79M)

The Global Combat Support System – Marine Corps (GCSS-MC) is a portfolio of systems that supports logistical elements of command and control, joint logistics interoperability, and secure access to and visibility of logistics data. GCSS-MC is based on the Marine Corps Logistics Operational Architecture and logistics business process reengineering initiatives. GCSS-MC is part of a joint GCSS effort that aims to improve logistics capability and fill in deficiencies in the accuracy and timeliness of logistics data.

GCSS-MC Logistics Chain Management (LCM) is a program within GCSS-MC comprised of Increments 1, 2, and 3. GCSS-MC LCM Increment 1 provides initial capabilities for GCSS-MC. The system provides Combat Service Support functionality: Supply, Maintenance, Task Organization, and Request Tracking in a shared data environment in support of deployed operations. Specifically, the system centralizes logistics information for access by multiple authorized users (closing a significant warfighting gap), complies with the J-4 GCSS Mission Area Interface Control Document that establishes a DoD Family of Systems for logistics information visibility and decision support, and satisfies initial Marine Corps requirements for meeting Combatant Commander 129/57 Data Elements that provide asset visibility data to Combatant and Joint Task Force Commanders.

FY17 funds will be used in Operations and Maintenance, so that the Marine Corps funding will support GCSS-MC/LCM Increment 1 sustainment currently supported by SPAWAR System Center Atlantic as well as GCSS-MC Program Management Office support contractor (Island Creek Associates). FY17 funds in Research and Development will enable Oracle Business Suite R12 Refresh (Lockheed Martin) to complete refresh activities.

E. Human Resource Management

Top 5 Investments within Segment	***FY17 ($M)***
Integrated Personnel And Pay System-Army Increment 2	*$165*
Military Entrance Processing Command Integrated Resource System	*$93*
Defense Enrollment Eligibility Reporting System	*$75*
Real-Time Automated Personnel Identification System And Common Access Card	*$64*
Defense Civilian Personnel Data System	*$53*

Integrated Personnel And Pay System-Army Increment 2 (FY17 $165M)

Integrated Personnel and Pay System (IPPS) –Army Increment II will deliver fully integrated personnel and pay services for all Army Components that builds on the trusted database delivered by the IPPS-A Increment I program. Increment II will link the personnel and pay functions for all Army personnel, eliminating duplicate data entry, reducing complex system maintenance, and minimizing pay discrepancies. IPPS-A Increment II will account for status changes between Active, Reserve, and National Guard components, to ensure accurate service time and minimize impact on individual pay, credit for service, and other benefits, as well as enable disciplined human resource management. This will support DoD IT priority of managing DoD data.

FY17 funds will field IPPS-A, to include New Equipment Training (NET), as well as procurement of hardware and software that is required to build out the infrastructure of IPPS-A Data Centers. Funds will also provide the completion of the Primary Design Review and Critical Design Review for the entire Increment and begin the design, development, integration, and testing activities for Release 2.0. Release 2.0 activities include data call from legacy systems, data analysis, data cleansing, and data conversion; design and build of the system technical architecture for IPPS-A; and Enterprise Resource Planning system configuration against functional personnel specifications. Finally, FY17 funds will support the IPPS-A Increment II functionalities, such as civilian salaries, program office contractor support, data center support, travel and training for program office personnel, software license renewal, and Help Desk support.

Military Entrance Processing Command Integrated Resource System (FY17 $93M)

U.S. Military Entrance Processing Command Integrated Resource System (USMEPCOM MIRS): MIRS provides the automation and communications capability for USMEPCOM to meet its peacetime, mobilization, and wartime military manpower accession mission for the Armed Services. USMEPCOM conducts its work through 65 Military Entrance Processing Stations (MEPS) across the country. The main objectives of these 65 MEPS is to conduct aptitude tests, medical examinations, and administratively process; enlist, and ship applicants for the Armed Forces and Reserves; conduct aptitude tests, medical examinations and determine acceptability, administratively process, allocate, induct and ship Selective Service System registrants, when required; and provide aptitude and medical examination services for other Federal agencies, as requested. MIRS interfaces with recruiting capabilities for the services, incorporating the concept of electronic data sharing using standard Department of Defense (DoD) data elements between USMEPCOM and all the Armed Services recruiting and accession commands. In the event of a required military draft, MIRS would directly support mobilization through electronic links with the Selective Service system and its ability to provide processing and shipment to boot camp capability for those drafted into military service.

FY17 USMEPCOM will use funds to:

- Maintain MIRS, associated network infrastructure, and Applicant Processing Systems to meet DoD and Army Certification and Accreditation requirements and changes to enlistment standards, including changes to applicable law
- Complete consolidation of MEPS servers to HQ Data Center and Oracle 11g upgrade efforts
- Initiate MIRS application update to include effort to implement Common Access Card (CAC) single-sign-on capability to protect applicant Personally Identifiable Information (PII) data
- Complete enterprise applicant processing COOP location to meet requirement due to consolidation, centralization and virtualization of MIRS servers/databases from 66 geographically separated locations to a single location
- Initiate technology refresh of MEPS PBX and Voicemail systems with Voice over Internet Protocol
- Continue implementation of workflow and business rule engines

Defense Enrollment Eligibility Reporting System (FY17 $75M)

Defense Enrollment Eligibility Reporting System (DEERS) serves as DoD's only authoritative data repository of all manpower, personnel (military, civilian, selected contractors, retirees, and family members), benefit eligibility, and TRICARE enrollments worldwide. DEERS provides and maintains medical and personnel readiness information on Uniformed Services members, DoD and Medicare eligibility status, Federal Service member's Group Life Insurance enrollment, and it also serves as the central repository for immunizations and the single portal for DoD benefit information. The program maintains enrollment and eligibility verification data from existing DEERS client applications and interfacing systems, as well as the DoD Components and non-DoD information systems. In addition, the DEERS Person Data Repository (PDR) maintains records for more than 39 million persons.

DEERS provides hundreds of system interfaces, web services, and applications to the military healthcare systems. DEERS is designed to add enterprise solutions quickly and efficiently, resulting in better, more cost effective service to members and warfighters. DEERS serves as the source of eligibility for benefits and entitlements.

FY17 funds will be used in the following appropriations to support:

- Operations and Maintenance (O&M):
  - Assisting Veterans Affairs by providing Service information to enable VA improvements in disability claims processing and reduce veterans' wait-time; automating the DD214 separation document; automating life insurance designations for service members; and updating reporting requirements for the Internal Revenue Service (IRS) to verify minimal essential coverage compliance with the Affordable Care Act. In addition, O&M funding will be utilized in the following activities:
    - Development and execution of enrollment, operations, and customer service improvements, as well as the security mandates, management controls and transition requirements for the TRICARE Dental and TRICARE East and West Regions (medical) programs
    - Continued development and expansion of the Defense Manpower Data Center (DMDC) portal, focusing on creating a "one-stop" place for beneficiaries to get benefits and DoD-related information and transform customer service through migration to electronic mechanisms, including e-Correspondence, mobile applications, milConnect, and other self-service capabilities
  - Continue to provide 1.7 billion identity web service transactions with sub second response times for both the NIPR and SIPR customers.
- Procurement: FY17 investments will be used to purchase additional identity proofing's from a vendor that allows the user's credential to be issued online (remotely) simplifying the process for the Beneficiary by avoiding the necessity to be in-person proofed and reducing the cost for the Government by avoiding the costs associated with in-person proofing (manpower, facility, mailings). These identity proofings will further be utilized to allow a Beneficiary to reset the password when he or she has forgotten the username, password and challenge questions. This avoids the much higher costs associated with calls to a help desk, and provides our Beneficiaries with immediate resolution.

Real-Time Automated Personnel Identification System And Common Access Card (FY17 $64M)

Real-Time Automated Personnel Identification System (RAPIDS) is the infrastructure that supports the Uniformed Services identification card, provides on-line updates to DEERS, and issues the Common Access Card (CAC) to Service members, civilian employees, and eligible contractors. As the identification card for Service members, civilian employees, and eligible contractors, the CAC provides the enterprise-wide credential for both physical and logical access to DoD facilities and networks. CAC uses the DEERS database for authentication and personnel information.

The RAPIDS program is a network of over 2,475 issuing stations at approximately 1,695 locations providing the seven Uniformed Services the means to verify eligibility for benefits and entitlements. CAC is essential to the Department's enterprise-wide solution for secure identity credentialing by allowing logical access to DoD computer networks and systems, as well as physical access to buildings and secure areas.

FY17 funds will be used in the following appropriations to support:

- Operations and Maintenance (O&M):
  - Provides and maintains the ability to issue the definitive identity credential of affiliation with the DoD. It relies on the information stored in the DEERS Person Data Repository (PDR)
  - Enables design of increased security features into future versions of the CAC and Uniformed Services Identification (USID) cards produced from RAPIDS that will reduce fraud and counterfeiting
  - Maintains an average issuance time of no more than 17 minutes for all DoD Identification cards, and 97 percent availability for the RAPIDS system
  - Continued identity verification for authorized personnel to manage entry and movement within DoD Installations, buildings, or facilities; regulate access to DoD computer systems and network; and verify eligibility, if authorized, for DoD benefits and privileges
- Research Development Test and Evaluation (RDT&E): Investment funding sources the following activities:
  - Provides security personnel notices on persons of interest attempting to access facilities, and increased personnel protection and policy compliance
  - Provides for the continued acquisition, installation, and maintenance of the DMDC RAPIDS/CAC infrastructure, as well as replacing outdated and/or maintenance-intensive equipment in order to continue to ensure full functionality, system security, and HSPD-12 implementation

Defense Civilian Personnel Data System (FY17 $53M)

The Defense Civilian Personnel Data System (DCPDS) is the Department's enterprise civilian HR automated system that supports one-third of the federal work force. Network operations span worldwide and are online 24/7. DCPDS architecture is standardized for all enterprise servers and all Military Departments and Defense Agency regional platforms and uses commercial-off-the-shelf (COTS) hardware and software. DCPDS has migrated to Oracle's Release 12 software, ensuring the technology base to maintain DCPDS as a continued leader in federal HR systems. Web-enabled DCPDS and the addition of its Self Service capability have increased the number of users from 20,000 HR specialists to more than 800,000 DoD employees. Led by the Defense Civilian Personnel Advisory Service (DCPAS), the DCPDS manager, the Office of Management and Budget (OMB) and the Office of Personnel Management (OPM) have designated the Department as one of six (6) HR Shared Service Centers. DCPDS has proved its business case and saves the Department over $200 million per year by operating centrally those HR system activities previously operated by the individual Services/Defense Agencies. The future focus of DCPDS is consolidation of all DCPDS regional operations to a single site. Enterprise operations, as well as several DoD Component customers' regional operations, are currently located at a DCPDS central site. DCPAS has managed the development, deployment, and administration of the DCPDS operation. DCPDS operational activities include processing of all personnel transactions, providing workforce analysis and reporting for DoD and external government agencies, supporting health insurance programs, managing benefits, and reporting certification and training. DCPDS supports the entire civilian HR lifecycle, with transactions and information that reflect acquiring, assigning, training and development, sustaining and managing HR compensation, managing organizations, supporting benefits management, and separation or termination of civilian personnel. Reporting includes leadership-level corporate reporting across the enterprise, as well as individual Military Department and Defense Agency customer information. This investment directly supports the strategic goals of the DoD HR Strategic Plan, developing and implementing innovative HR management solutions that enable the DCPDS customer –leaders, managers, and employees throughout the Department – to ensure the DoD civilian workforce is able to effectively support the Warfighter and the national security mission. FY17 funds will be used to:

- Implement initial cloud computing, improve data warehouses, and continue expansion of web services
- Enhance information assurance and cybersecurity requirements, including demilitarized zone (DMZ) extension mandates
- Develop enhancements to comply with HR legislative and DoD regulatory requirements
- Support required changes for HR Line of Business (LoB) interfaces and other OPM/OMB mandates

F. Health

Top 5 Investments within Segment	*FY17 ($M)*
Department Of Defense Healthcare Management System Modernization	*$458*
Armed Forces Health Longitudinal Technology Application	*$138*
Defense Medical Information Exchange	*$57*
Composite Health Care System	*$54*
Executive Information/Decision Support	*$50*

Health Segment Overview

The integrated Military Health System (MHS) is composed of direct care provided in over 400 military treatment facilities and care purchased through civilian providers and institutions. Extending from theater medical care for deployed forces to the daily delivery of "peacetime" health services, it delivers a coordinated continuum of preventive and curative services for the 9.4 million members of the DoD health care beneficiary population and is accountable for health outcomes and cost while supporting the Services' warfighter requirements.

MHS Health Information Technology (MHS HIT) is an integral part of the DHA's enterprise-focused organizational structure. MHS HIT manages IT shared services and is the oversight authority for IT-related expenditures, promoting greater accountability. The MHS HIT mission is to implement, manage, and sustain an integrated and protected medical information enterprise in order to ensure that the right information is accessible to the right customers at the right time and in the right way. HIT infrastructure and systems are critical enablers within the MHS.

For the largest investments within the DoD Health segment, two are legacy systems – Armed Forces Health Longitudinal Technology Application (AHLTA) and Composite Health Care System (CHCS). DoD Healthcare Management System Modernization (DHMSM), the largest FY17 investment request, is the upgrade to these legacy systems. DMIX program will acquire the capabilities necessary to securely and reliably exchange standardized, normalized, and correlated health data with all partners through standard data/information exchange mechanisms. DMIX manages the data exchange capability from legacy data stores in order to prepare for the transition to the modernized Electronic Health Record platform being acquired by DoD Healthcare Management System Modernization (DHMSM).

Finally, the Health Segment includes the Executive Information/Decision Support (EI/DS) business initiative, which receives and stores data from MHS systems, processes those data through a variety of business rules, and makes the data available, in various data marts, to managers, clinicians, and analysts for the management of the business of health care.

Department of Defense Healthcare Management System Modernization (FY17 $458M)

DoD Healthcare Management System Modernization (DHMSM) will acquire, deploy, and implement an electronic health record (EHR) system that replaces the DoD legacy MHS inpatient and outpatient EHR systems. The overarching goal of the program is to enable healthcare teams to deliver high-quality, safe, care and preventive services to patients through the use of easily accessible standards-based computerized patient records resulting in: improved accuracy of diagnoses and medication; improved impact on health outcomes; increased patient participation in the healthcare process; improved patient-centered care coordination; and increased practice efficiencies in all settings, including all DoD operational environments.

DHMSM will be executed to deliver uniform information management options across both garrison and theater environments. DHMSM will focus on the replacement of inpatient and outpatient systems, and will encompass deployment of the enterprise EHR to fixed facilities as well as expeditionary components. DHMSM will replace the DoD legacy healthcare management systems with a commercial off-the-shelf capability that is open, modular, and standards-based with non-proprietary interfaces. DHMSM will support the Department's goals of net- centricity by providing a framework for full human and technical connectivity and interoperability that allows DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and that also protects the information from those who should not have it. Once fielded, the EHR will support the following healthcare activities for DoD's practitioners and beneficiaries:

- Clinical workflow and provider clinical decision support
- Capture, maintenance, use, protection, preservation, and sharing of health data and information
- Retrieval and presentation of health data and information that is meaningful for EHR users regardless of where the patient's records are physically maintained
- Analysis and management

In FY17, the various appropriations will provide funding to complete system integration and operational testing to achieve Initial Operating Capability (IOC), purchase required software licenses and hardware, complete site readiness reviews and fielding to IOC sites and subsequent site installations, and conduct change management and user training. Additionally, funds will prepare analyses and documentation for Full Deployment Decision (FDD) Authorization to Proceed (ATP). Modernization of the DHMSM in conjunction with the VA will leverage IT to increase efficiency and effectiveness of healthcare, streamlining digital healthcare record management to improve the quality of patient care globally throughout the Department's medical enterprise.

Armed Forces Health Longitudinal Technology Application (FY17 $138M)

Armed Forces Health Longitudinal Technology Application (AHLTA) is the DoD's current EHR, and while also one of the world's largest clinical information systems, it is the enterprise foundation product for outpatient clinical documentation. AHLTA provides secure, 24x7, worldwide online access to patients´ medical records, making it a key enabler of military medical readiness. AHLTA stores data in a central location to ensure healthcare providers have ready access to medical information when and where needed to support the military's highly mobile patient population. It is envisioned that AHLTA will be replaced by the DHMSM. AHLTA stores data in a central location to ensure that healthcare providers have ready access to medical information when and where needed to support the military´s highly mobile patient population. As military members move from location to location, AHLTA is readily available to support their healthcare needs. AHLTA provides DoD healthcare providers with ready access to medical information when and where needed to support the military´s highly mobile patient population. Since the worldwide implementation of AHLTA in 2006, use of the system has grown at a significant pace. AHLTA processes an average of 155,000 encounters each workday, and more than 300 million outpatient encounters are stored in its clinical data repository. Patient encounter records are retrievable at nearly 450 fixed and deployed treatment facilities worldwide. The enterprise serves more than 9.4 million service members, retirees, and beneficiaries. This FY17 funding request includes:

- Data life cycle management and worldwide onsite support for resolving Patient Safety Issues and bug fixes
- Manage and sustain the current Military Health System's current EHR to provide optimal system upgrades focusing on operational availability, speed, and provider capabilities
- Complete deployment of AHLTA 3.3.9
- Complete the VB6 to .Net code conversion in AHLTA
- Sustain AWP 2.0 (Vendor Software Maintenance and DISA Sustainment)
- Complete CommVault Phase 2 (over the wire/remote backup capability for CommVault)

Defense Medical Information Exchange (FY17 $57M)

Defense Medical Information Exchange (DMIX) is comprised of the infrastructure and services needed to facilitate seamless, integrated sharing of electronic health data between DoD, VA, other Federal agencies, and industry partners that also is viewable to DoD and VA providers through a joint viewer.

DMIX program will acquire the capabilities necessary to securely and reliably exchange standardized, normalized, and correlated health data with all partners through standard data/information exchange mechanisms. This allows users in different places and different organizations to access, use, and supplement health data (technical interoperability) that has a shared meaning so that users (assisted by computers) are able to make care decisions. DMIX manages the data exchange capability from legacy data stores in order to prepare for the transition to the modernized EHR platform being acquired by DoD Healthcare Management System Modernization (DHMSM). DMIX consists of a family of capability initiatives supporting the seamless exchange of standardized health data among DoD, VA, and other Federal agencies; private providers; and benefits administrators. The DMIX program provides the capability for healthcare providers to access and view complete and accurate patient health records from a variety of data sources, therefore allowing healthcare providers to make faster and higher quality care decisions. DMIX was established in accordance with the joint memo from Under Secretary of Defense (Comptroller) (USD(C)) and USD (AT&L) titled "Joint Memorandum on Major Defense Acquisition Program and Major Automated Information System Program Resource Transparency in Department of Defense Budget Systems" dated June 27, 2013.

In addition, Joint Electronic Health Record Interoperability (JEHRI) and Virtual Lifetime Electronic Record (VLER) Health (to include Exchange) are part of the DMIX program as a direct result of the Acquisition Decision Memorandum (ADM) signed January 2, 2014 by the USD (AT&L). Use of the health data may be done via legacy systems, clinical mobile applications, and system-agnostic viewers, such as the Joint Legacy Viewer (JLV). Customers include the Military Health System (MHS), VA, other federal agencies and over 200,000 medical care practitioners.

FY17 funds will be used to:

- Continue to sustain the DMIX Data Exchange Services
- Continue to support DoD Healthcare Management System Modernization (DHMSM) deployment
- Sustain the DMIX Viewer component and underlying infrastructure necessary to ensure providers are able to view a patient's comprehensive health history via a single data display

Composite Health Care System (FY17 $54M)

Composite Health Care System (CHCS) is the military´s current computerized provider order entry (CPOE) system supporting Military Treatment Facilities worldwide associated with managing healthcare services through a beneficiary enrollment process. It enables healthcare providers to order tests, schedule services, and prescribe medication to 9.4 million service members, retirees, and beneficiaries. CHCS improves patient safety and enables improved quality of care. CHCS supports compliance with health plan coverage, reimbursement, benefit provisions, and necessary management support activities. Information in the health record, such as care plans, is standardized and easily accessed from multiple sites to meet the needs of a mobile population. Clinical documentation entered through the DoD EHR is sent to CHCS and its modules to provide the official repository of the medical coding information to handle the transmission of those encounters via interface. It is envisioned that CHCS will be replaced/sun set by the DoD Healthcare Management System Modernization.

FY17 funds will be used to:

- Provide for maintenance, legacy support, systems engineering, information assurance, licensing, and contracting fees; fund civilian salaries, program office contractor support, travel, and training for program office personnel; and continue on-site support to CONUS, European, and Pacific sites

- Continue to support the following medical Information Management/Information Technology (IM/IT) environment, including:
  - Patient administration
  - Patient appointments and scheduling
  - Managed care program
  - Clinical
  - Laboratory, Radiology, Pharmacy
  - Dietetics
  - Quality assurance
  - Workload accounting menu
  - Medical services accounting
  - Ambulatory data menu
  - Medical records tracking

Executive Information/Decision Support (EI/DS) (FY17 $50M)

EI/DS is comprised of a central data mart Military Health System Data Repository (MDR) and several smaller data marts, including:

- MHS Management Analysis and Reporting Tool (MART M2)
- Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE)
- Purchased Care Operations Systems -TRICARE Encounter Data (TED) & Patient Encounter Processing and Reporting (PEPR)

Many of these operate within a Business Objects XI (BOXI) environment. EI/DS manages receipt, processing, and storage of more than 155 terabytes of data from both Military Treatment Facilities (MTF) and the TRICARE purchased care network systems. These data include inpatient dispositions, outpatient encounters, laboratory, radiology, and pharmacy workload, TRICARE network patient encounter records, TRICARE mail order pharmacy patient encounter records, beneficiary demographics, MTF workload and cost information, eligibility and enrollment, Pharmacy Data Transaction Service data, customer satisfaction surveys, and data associated with the Wounded Warrior care. EI/DS provides centralized collection, storage, and availability of data, in various data marts, to managers, clinicians, and analysts for the management of the business of healthcare.

FY17 funds will be used to continue the sustainment and maintenance of applications, including program management, software upgrades, information assurance procedures, software maintenance fixes, testing & evaluation, and security accreditation. Additionally, with regard to the ESSENCE program:

- Expand data storage/maintenance/access from 18 months to five years for near-real-time health surveillance
- Implement geographic information system (GIS) capability within ESSENCE to display spatial detection results and point source of counts by patient's residence through heat maps
- Provide analysis of encounter-related laboratory positive results data to design specific case definitions and allow users to determine the proportion of Influenza-Like Illness (ILI) cases due to a specific pathogen
- Design (preliminary only) access and ingest denominator data to calculate rates for each syndrome or category

5. Classified SNAP IT Budget Submissions

The classified portion of the FY17 President's Budget Request is available electronically on Compact Disk. Additionally, electronic copies of the same notebook can be found on the Secret Internet Protocol Router Network (SIPRNet) at the following location:

https://snap.pae.osd.smil.mil/snapit/Home.aspx

6. Electronic-Government (eGovernment)

eGovernment

DoD has benefited from 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 and IT Portfolio Management, IT Consolidation, and Information Management / Information Technology / Information Assurance (IM/IT/IA) workforce development. The following initiatives will be funded by DoD agency contributions[1] in FY17.

Initiative / Line of Business (LoB)	FY16	FY17
Budget Formulation and Execution LoB	$105,000	$110,000
E-Rulemaking	$73,912	$89,024
Federal Health Architecture LoB	$2,656,000	$2,656,000
Financial Management LoB	$187,342	$207,300
Geospatial LoB	$225,000	$225,000
Grants.gov	$584,477	$704,902
Human Resources Management LoB	$260,870	$260,870
Integrated Award Environment	$31,889,691	$25,909,983
Performance Management LoB	$53,000	$79,800
Security, Suitability, and Credentialing LoB	$0	$2,000,000
USAJOBS	$952,213	$775,181
DoD Total	**$36,987,505**	**$33,018,060**

[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.

Objective of eGovernment Initiatives / LoBs:

Budget Formulation and Execution LoB / Managing Partner, Department of Education - The Budget Formulation and Execution LoB (BFE LoB) provides agencies with technological solutions, tools, and services for enhanced budgeting, analysis, document production, and data collection. The BFE LoB also provides tools for secure collaboration and online meetings, and human capital solutions. Through the BFE LoB, agencies can share best practices for budgeting activities, identify training and educational opportunities, and communicate core competencies and career path options for budget analysts. Finally, the BFE LoB provides governance solutions, supporting year-round coordination via a program management office, furthering the idea of sharing and reuse, and setting standards for data and data exchange.

E-Rulemaking / Managing Partner, Environmental Protection Agency - E-Rulemaking provides citizens with one access point to view and comment on rules and notices. This program and its supporting application allow agencies to fulfill the E-Government Act of 2002 requirement to ensure a publicly accessible website containing electronic dockets for regulations. The E-Rulemaking program includes two important components: (1) Regulations.gov: the public website that provides citizens, small businesses, educators, multinational corporations, civic organizations, and all levels of government with one-stop Internet access to view, download, and submit comments on all Federal regulations. Agencies are required to ensure their public regulatory dockets are electronically accessible and searchable using Regulations.gov and to accept electronic submissions via the website. (2) Federal Docket Management System (FDMS): an advanced "back-end" docket management system that provides Department and Agency staff with improved internal docket management functionality and the ability to publicly post all relevant documents on Regulations.gov (e.g., Federal Register documents, proposed rules, notices, supporting analyses, and public comments).

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.

Financial Management LoB / Managing Partner, Department of the Treasury – The vision of the Financial Management LOB (FMLoB) is to create government-wide financial management solutions that are efficient and that improve business performance, while ensuring integrity in accountability, financial controls, and mission effectiveness. FMLoB 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. A benefit for most agencies will be a new synergy and coordination of top-down policy and guidance across these domains, allowing agencies to streamline operations in more standardized manner.

Geospatial LoB / Managing Partner, Department of the Interior – This LoB provides cross-agency coordination, and identifies opportunities for optimizing and consolidating Federal geospatial-related investments. The Geospatial LoB (Geo LoB) seeks to improve sharing of geospatial information, and reduce costs by avoiding the creation of duplicative geospatial information. The Geo LoB also enables partner agencies to collaborate and apply geospatial information, and provides services to support national defense priorities. Sharing data, services, and applications through the Geo LoB lowers costs for data, hardware, and software, which increases the volume of data shared with the public. The Geo LoB also helps the geospatial community continue to serve as leaders in the implementation of publishing services for open government data.

Grants.gov / Managing Partner, Department of Health and Human Services - Grants.gov provides a single website to find and apply for federal discretionary grants. Grants.gov provides over one million organizations with a single web site where they can find and apply for over $153 billion worth of grants distributed annually. Grants.gov empowers smaller agencies with limited resources to improve the reach of their grant programs, and provides larger agencies with the benefit of process standardization, cost savings, and increased visibility. The program is funded by the twenty-six Federal grant-making agencies, each providing support commensurate with its size according to a formula approved by the Council on Financial Assistance Reform (COFAR).

Human Resources LoB / Managing Partner, Office of Personnel Management – The DOD is one of the approved service providers for the Human Resources LoB (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 (DCPAS) and the Defense Finance and Accounting Service (DFAS). 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.

Integrated Award Environment / Managing Partner, General Services Administration (GSA) – The Integrated Award Environment (IAE) is a Presidential E-Government initiative managed by GSA. The IAE uses innovative processes and technologies to improve systems and operations for those who award, administer, or receive federal financial assistance, such as grants or loans, contracts, and intergovernmental transactions. The Integrated Award Environment manages ten federal IT systems that enable searching for, applying for, and tracking federal awards, as well as registration capabilities to engage in the process.

Performance Management LoB / Managing Partner, GSA – The Performance Management Line of Business (PMLoB) is an interagency effort to develop government-wide performance management capabilities to help meet the transparency requirements of the Government Performance and Results Modernization Act of 2010 (GPRAMA), and support government-wide performance management efforts. The creation of the PMLoB was approved by the Director of OMB in November 2011. Key Objectives of the PMLoB include:

- Develop Performace.gov into a GPRAMA-compliant tool, including providing flexible solutions to meet GPRAMA machine-readability and Federal Program Inventory requirements
- Develop flexible and balanced approaches to provide OMB, Congress, and others with a cohesive view of federal performance, while allowing individual agencies to provide specific performance information and perspective facilitating stakeholder understanding in a cost effective manner
- Examine opportunities to leverage Performance.gov to streamline Agency reporting to OMB, OMB/Congressional reviews, and maximize workload efficiency and minimize burden
- Provide a government-wide capacity that complements agency performance management activities and systems in a cost effective manner

Security, Suitability, and Credentialing LoB, Managing Partner, Office of Personnel Management - The Suitability and Security Clearance Performance Accountability Council (PAC) Program Management Office's (PMO) mission is to enable the PAC's ability to drive reforms to the Executive branch's security clearance, suitability/fitness, and credentialing processes. The PAC PMO also serves the Program Management Office function for the Security, Suitability, and Credentialing Line of Business (SSCLoB). The SSCLoB's vision is to facilitate Executive branch-wide, modern, cost-effective, standardized, and interoperable personnel security, suitability, and credentialing solutions, providing common, core functionality to support the strategic management of this LoB.

USAJOBS / Managing Partner, Office of Personnel Management - The USAJOBS.gov website provides a place where citizens can easily search for employment opportunities throughout the Federal Government. USAJOBS is a fully operational, state-of-the art recruitment system that simplifies the Federal job search process for both job seekers and agencies. USAJOBS.gov provides users with access to: A centralized repository for all competitive service job vacancies; a resume repository used by agencies to identify critical skills; a standardized online recruitment tool and services; a standard application Process; and intuitive job searches, including e-mail notifications for jobs of interest.

7. FITARA Statements

A. (U) The Chief Information Officer of the Department of Defense (a) reviewed and provided recommendations to the Secretary of Defense on the information technology budget request of the Department, and (b) certifies that information technology investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget.

B. (U) The CFO and CIO jointly affirm that the CIO had a significant role in reviewing planned IT support for major programs and significant increases and decreases in IT resources

8. Conclusion

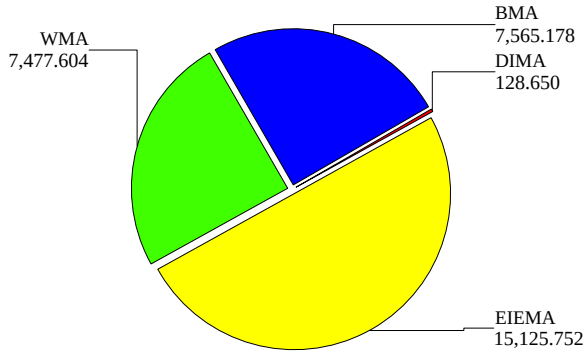
As Secretary Carter remarked while previewing the Department's 2017 budget at the Economic Club of Washington on February 2nd, today's security environment is dramatically different than the environment in which we have engaged for the last twenty-five years, and it requires new ways of thinking and new ways of acting. In a world of constantly changing cybersecurity challenges, the Department's IT remains increasingly at the forefront of this complex security environment. Taking the long view, the Department is driving technological innovation in the FY17 budget to stay ahead of future threats over the long term, and keep the U.S. military the best in the world. Focused on IT priorities that will drive security, efficiency, and effectiveness in the Department's networks and systems, the DoD IT budget is poised to keep the Department's IT on this path to progress during the upcoming fiscal year.

The DoD fiscal year 2017 total IT budget request is $38.2B, representing a $1.4B (3.9%) increase from the fiscal year 2015 enacted budget. This includes both unclassified ($30.3B) and classified ($7.9B) investments. Pursuing the Department's IT priorities will improve the security, efficiency, and effectiveness of DoD IT by modernizing the networks, sharing with mission partners, managing DoD data, defending against cyber-attack, and empowering mobile data access.

9. Appendix

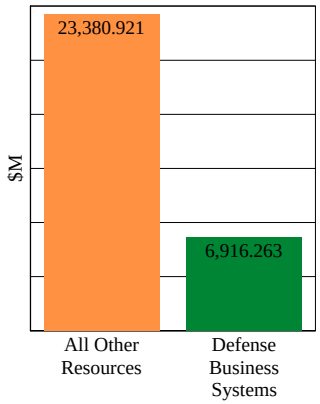
**DoD INFORMATION TECHNOLOGY BUDGET REQUEST
SUMMARY
(DOLLARS IN MILLIONS)**

Mission Area



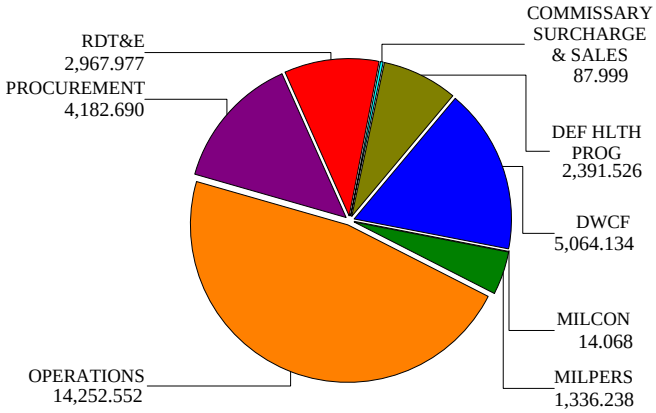
FY2017 ($M)

Business System Breakout



FY2017 ($M)

Appropriation



FY2017 ($M)

FY16 to FY17 Comparison ($M)

	FY2016	Inflation	Program Change	FY2017
PB FY2017:	30,780.245	523.256	-483.061	30,297.184

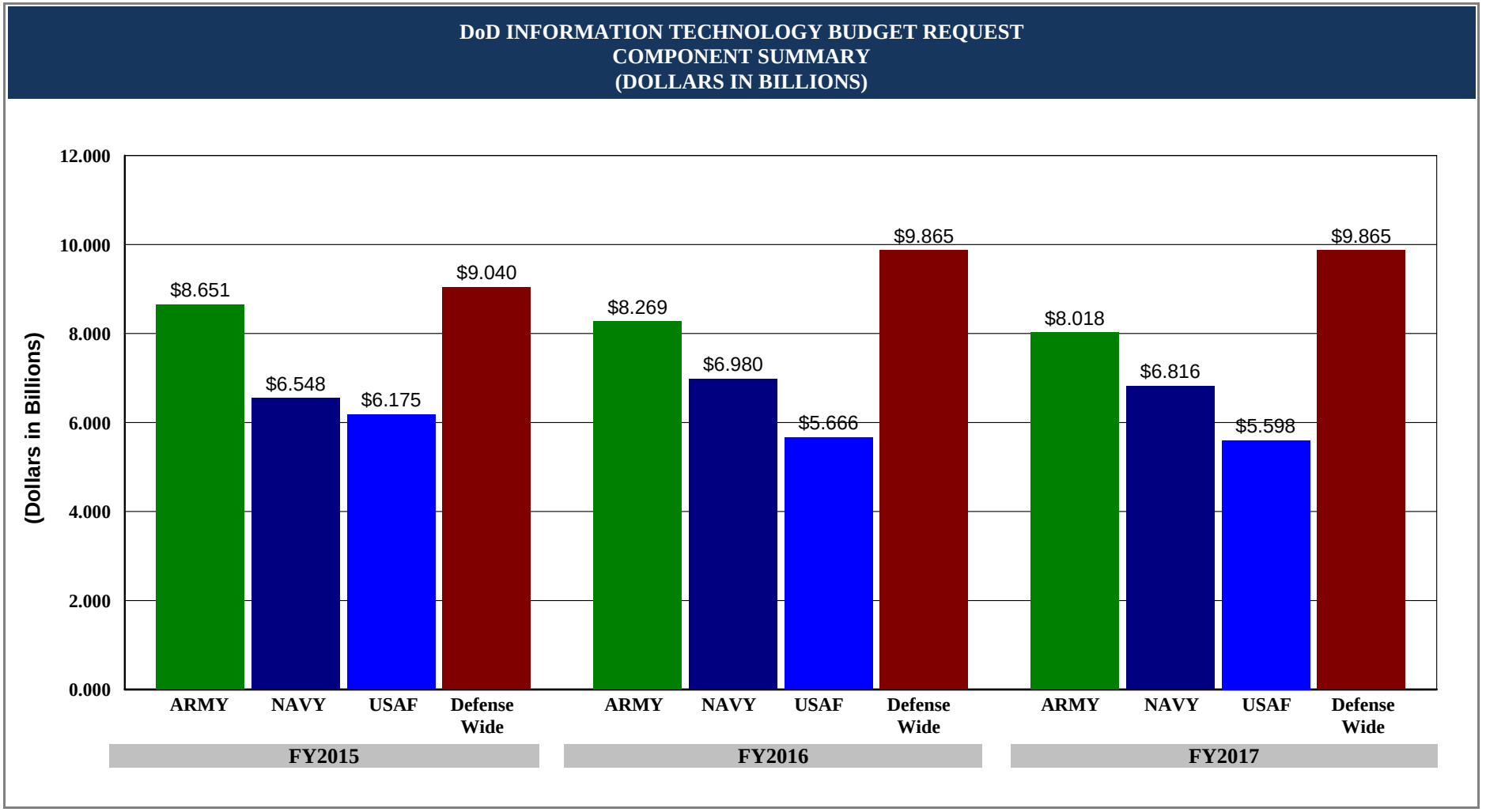
FY16/FY17PB Comparison ($M)

	FY2016	FY2017	Delta
PB FY2016:	30,467.336	30,519.258	51.922
PB FY2017:	30,780.245	30,297.184	
Delta:	312.909	-222.074	

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY DEPARTMENT (DOLLARS IN MILLIONS)			
DEPARTMENT	**FY2015**	**FY2016**	**FY2017**
DEPARTMENT OF ARMY	$8,650.985	$8,269.274	$8,018.146
DEPARTMENT OF NAVY	$6,547.940	$6,980.128	$6,816.067
DEPARTMENT OF AIR FORCE	$6,174.968	$5,665.974	$5,597.831
DEFENSE WIDE ACTIVITIES	$9,040.379	$9,864.869	$9,865.140
DOD TOTALS	**$30,414.272**	**$30,780.245**	**$30,297.184**

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
$8.651
$6.548
$6.175
$9.040
$8.269
$6.980
$5.666
$9.865
$8.018
$6.816
$5.598
$9.865
ARMY
NAVY
USAF
Defense Wide
FY2015
FY2016
FY2017

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY COMPONENT (DOLLARS IN MILLIONS)			
	FY2015	**FY2016**	**FY2017**
GRAND TOTAL	**$30,414.272**	**$30,780.245**	**$30,297.184**
DEPARTMENTS	**$21,373.893**	**$20,915.376**	**$20,432.044**
ARMY	$8,650.985	$8,269.274	$8,018.146
NAVY	$6,547.940	$6,980.128	$6,816.067
AIR FORCE	$6,174.968	$5,665.974	$5,597.831
DEFENSE AGENCIES	**$8,150.521**	**$8,967.566**	**$8,910.128**
DARPA	$35.160	$35.645	$37.285
DCAA	$29.352	$30.491	$36.804
DCMA	$127.517	$123.975	$124.391
DeCA	$89.280	$141.220	$176.183
DFAS	$347.900	$400.566	$372.280
DHA	$1,924.376	$2,355.885	$2,391.526
DISA	$2,709.549	$2,867.355	$2,941.471
DLA	$1,509.071	$1,566.357	$1,318.241
DPAA	$7.608	$15.767	$15.907
DSCA	$15.095	$13.662	$12.947
DSS	$35.818	$38.606	$38.346
DTRA	$112.823	$114.045	$126.884
JCS	$101.413	$94.852	$120.700
MDA	$232.526	$238.751	$234.080
OSD	$181.932	$143.781	$145.023
PFPA	$34.999	$37.357	$36.501
SOCOM	$246.675	$291.524	$307.885
TRANSCOM	$409.427	$457.727	$473.674
FIELD ACTIVITIES	**$889.858**	**$897.303**	**$955.012**
DCMO	$4.833	$5.000	$0.000

BY COMPONENT - continued (DOLLARS IN MILLIONS)			
	FY2015	**FY2016**	**FY2017**
DHRA	$287.066	$296.905	$315.687
DMACT	$81.391	$68.597	$82.884
DODEA	$153.905	$157.928	$161.430
DTIC	$21.501	$23.384	$22.851
DTSA	$5.132	$4.386	$5.537
IG	$39.287	$37.138	$42.403
NDU	$20.957	$21.947	$23.085
WHS	$275.786	$282.018	$301.135

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

SEGMENT	FY2015	FY2016	FY2017
ACQUISITION	$488.170	$475.834	$467.996
BATTLESPACE AWARENESS-ENVIRONMENT	$205.269	$211.116	$201.937
BATTLESPACE AWARENESS-ISR	$84.661	$75.273	$128.650
BATTLESPACE NETWORKS	$2,867.464	$2,804.581	$2,903.133
BUILDING PARTNERSHIPS	$91.672	$91.109	$88.476
BUSINESS SERVICES TBD	$149.771	$142.101	$143.200
COMMAND & CONTROL	$2,731.478	$2,613.650	$3,137.377
CORE MISSION TBD	$136.435	$165.181	$122.629
DOD IT INFRASTRUCTURE	$14,996.686	$14,577.038	$13,810.424
FINANCIAL MANAGEMENT	$781.046	$900.239	$773.499
FORCE APPLICATION	$614.271	$475.177	$469.713
FORCE MANAGEMENT	$122.875	$132.900	$116.022
FORCE TRAINING	$216.844	$253.765	$250.823
HEALTH	$979.606	$1,375.966	$1,356.180
HUMAN RESOURCE MANAGEMENT	$1,699.090	$1,939.182	$1,997.323
INSTALLATION SUPPORT	$303.583	$325.048	$313.419
IT MANAGEMENT	$1,115.828	$1,221.217	$1,315.328
LOGISTICS/SUPPLY CHAIN MANAGEMENT	$2,665.821	$2,813.786	$2,513.561
PROTECTION	$163.702	$187.082	$187.494
DOD TOTALS	**30,414.272**	**30,780.245**	**30,297.184**

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST SEGMENTS BY COMPONENT (DOLLARS IN MILLIONS)			
ACQUISITION	**FY2015**	**FY2016**	**FY2017**
ARMY	$63.511	$45.103	$41.403
NAVY	$212.884	$203.338	$203.517
AIR FORCE	$71.328	$71.528	$74.516
DEFENSE WIDE	$140.447	$155.865	$148.560
	$488.170	$475.834	$467.996
BATTLESPACE AWARENESS-ENVIRONMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$55.386	$20.823	$14.185
NAVY	$69.598	$79.203	$81.161
AIR FORCE	$80.285	$111.090	$106.591
	$205.269	$211.116	$201.937
BATTLESPACE AWARENESS-ISR	**FY2015**	**FY2016**	**FY2017**
ARMY	$1.090	$1.012	$0.000
NAVY	$61.612	$56.686	$96.426
AIR FORCE	$21.959	$17.575	$32.224
	$84.661	$75.273	$128.650
BATTLESPACE NETWORKS	**FY2015**	**FY2016**	**FY2017**
ARMY	$1,091.115	$1,043.769	$1,058.729
NAVY	$622.797	$581.414	$556.332
AIR FORCE	$590.720	$637.423	$756.880
DEFENSE WIDE	$562.832	$541.975	$531.192
	$2,867.464	$2,804.581	$2,903.133
BUILDING PARTNERSHIPS	**FY2015**	**FY2016**	**FY2017**
ARMY	$0.997	$1.443	$0.718
AIR FORCE	$73.652	$74.358	$72.730
DEFENSE WIDE	$17.023	$15.308	$15.028
	$91.672	$91.109	$88.476

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
BUSINESS SERVICES TBD	**FY2015**	**FY2016**	**FY2017**
ARMY	$0.001	$0.000	$0.000
NAVY	$99.433	$79.921	$88.691
AIR FORCE	$27.399	$27.706	$28.359
DEFENSE WIDE	$22.938	$34.474	$26.150
	$149.771	$142.101	$143.200
COMMAND & CONTROL	**FY2015**	**FY2016**	**FY2017**
ARMY	$364.281	$362.614	$391.866
NAVY	$595.969	$475.603	$580.346
AIR FORCE	$1,337.024	$1,299.474	$1,690.285
DEFENSE WIDE	$434.204	$475.959	$474.880
	$2,731.478	$2,613.650	$3,137.377
CORE MISSION TBD	**FY2015**	**FY2016**	**FY2017**
ARMY	$9.077	$13.506	$12.084
NAVY	$48.501	$74.705	$61.394
AIR FORCE	$75.951	$73.580	$45.210
DEFENSE WIDE	$2.906	$3.390	$3.941
	$136.435	$165.181	$122.629
DOD IT INFRASTRUCTURE	**FY2015**	**FY2016**	**FY2017**
ARMY	$4,943.408	$4,407.869	$4,245.382
NAVY	$2,937.713	$3,279.227	$2,973.565
AIR FORCE	$2,601.446	$2,105.833	$1,649.388
DEFENSE WIDE	$4,514.119	$4,784.109	$4,942.089
	$14,996.686	$14,577.038	$13,810.424
FINANCIAL MANAGEMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$113.000	$118.457	$110.995
NAVY	$134.795	$157.339	$164.984
AIR FORCE	$161.353	$203.345	$110.699
DEFENSE WIDE	$371.898	$421.098	$386.821
	$781.046	$900.239	$773.499

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
FORCE APPLICATION	**FY2015**	**FY2016**	**FY2017**
ARMY	$250.230	$189.457	$181.015
NAVY	$23.285	$13.644	$5.331
AIR FORCE	$306.690	$233.107	$247.165
DEFENSE WIDE	$34.066	$38.969	$36.202
	$614.271	$475.177	$469.713
FORCE MANAGEMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$20.958	$19.965	$16.872
NAVY	$31.502	$39.231	$28.395
AIR FORCE	$62.380	$63.829	$61.058
DEFENSE WIDE	$8.035	$9.875	$9.697
	$122.875	$132.900	$116.022
FORCE TRAINING	**FY2015**	**FY2016**	**FY2017**
ARMY	$167.953	$186.823	$195.138
NAVY	$9.210	$12.108	$10.460
AIR FORCE	$31.169	$39.991	$38.610
DEFENSE WIDE	$8.512	$14.843	$6.615
	$216.844	$253.765	$250.823
HEALTH	**FY2015**	**FY2016**	**FY2017**
NAVY	$5.910	$5.042	$5.765
DEFENSE WIDE	$973.696	$1,370.924	$1,350.415
	$979.606	$1,375.966	$1,356.180
HUMAN RESOURCE MANAGEMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$567.874	$771.740	$801.034
NAVY	$399.555	$416.193	$452.731
AIR FORCE	$189.971	$177.306	$179.012
DEFENSE WIDE	$541.690	$573.943	$564.546
	$1,699.090	$1,939.182	$1,997.323

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
INSTALLATION SUPPORT	**FY2015**	**FY2016**	**FY2017**
ARMY	$128.775	$144.658	$132.973
NAVY	$79.500	$88.258	$90.980
AIR FORCE	$84.221	$82.184	$80.062
DEFENSE WIDE	$11.087	$9.948	$9.404
	$303.583	$325.048	$313.419
IT MANAGEMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$62.872	$57.522	$47.335
NAVY	$487.487	$601.665	$623.701
AIR FORCE	$11.699	$11.679	$11.819
DEFENSE WIDE	$553.770	$550.351	$632.473
	$1,115.828	$1,221.217	$1,315.328
LOGISTICS/SUPPLY CHAIN MANAGEMENT	**FY2015**	**FY2016**	**FY2017**
ARMY	$759.882	$816.479	$693.392
NAVY	$704.818	$788.392	$775.123
AIR FORCE	$420.672	$405.822	$382.238
DEFENSE WIDE	$780.449	$803.093	$662.808
	$2,665.821	$2,813.786	$2,513.561
PROTECTION	**FY2015**	**FY2016**	**FY2017**
ARMY	$50.575	$68.034	$75.025
NAVY	$23.371	$28.159	$17.165
AIR FORCE	$27.049	$30.144	$30.985
DEFENSE WIDE	$62.707	$60.745	$64.319
	$163.702	$187.082	$187.494
DoD Totals	**$30,414.272**	**$30,780.245**	**$30,297.184**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY MISSION AREA (DOLLARS IN MILLIONS)			
MISSION AREA	**FY2015**	**FY2016**	**FY2017**
BUSINESS	$7,067.087	$7,972.156	$7,565.178
DEFENSE INTELLIGENCE	$84.661	$75.273	$128.650
ENTERPRISE INFORMATION ENVIRONMENT	$16,112.514	$15,798.255	$15,125.752
WARFIGHTING	$7,150.010	$6,934.561	$7,477.604
DOD TOTALS	**$30,414.272**	**$30,780.245**	**$30,297.184**

Page left intentionally blank