Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Defense Advanced Research Projects Agency	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
Total Program Element	-	348.530	399.597	334.407	-	334.407	339.844	336.689	339.393	359.413	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	85.540	72.028	39.800	-	39.800	54.598	50.746	77.406	78.746	-	-
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	169.595	189.238	187.925	-	187.925	200.009	204.404	204.788	206.128	-	-
IT-04: *LANGUAGE TECHNOLOGY*	-	59.650	70.482	39.333	-	39.333	50.223	81.539	57.199	74.539	-	-
IT-05: *CYBER TECHNOLOGY*	-	33.745	67.849	67.349	-	67.349	35.014	-	-	-	-	-

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Information and Communications Technology program element is budgeted in the applied research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies.

The High Productivity, High-Performance Responsive Architectures project is developing the necessary computing hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include supercomputer, embedded computing systems, and novel design tools for manufacturing of defense systems.

The Information Assurance and Survivability project is developing the technology required to make emerging information system capabilities (such as wireless and mobile code/mobile systems) inherently secure, and to protect DoD's mission-critical systems against attack upon or through the supporting information infrastructure. These technologies will enable our critical systems to provide continuous correct operation even when they are attacked, and will lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites.

The Language Technology project will develop and test powerful new Human Language Technology that will provide critical capabilities for a wide range of national security needs. This technology will enable systems to a) automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means; b) to have two-way (foreign-language-to-English and English-to-foreign-language) translation; c) enable automated transcription and translation of foreign speech and text along with content summarization; and d) enable exploitation of captured, foreign language hard-copy documents.

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Defense Advanced Research Projects Agency	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*

The Cyber Technology project supports long term national security requirements through the development and demonstration of technology to increase the security of military information systems. This involves networking, people, platforms, weapons sensors, and decision aids to create a whole that is greater than the sum of its parts. The results are networked forces that operate with increased speed and synchronization and are capable of achieving massed effects without the physical massing of forces as required in the past.

B. Program Change Summary ($ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	392.421	413.260	393.462	-	393.462
Current President's Budget	348.530	399.597	334.407	-	334.407
Total Adjustments	-43.891	-13.663	-59.055	-	-59.055
• Congressional General Reductions	-0.519	-0.663			
• Congressional Directed Reductions	-40.734	-15.000			
• Congressional Rescissions	-	-			
• Congressional Adds	10.000	2.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-2.464	-			
• SBIR/STTR Transfer	-10.174	-			
• TotalOtherAdjustments	-	-	-59.055	-	-59.055

Change Summary Explanation

FY 2013: Decrease reflects Congressional reductions for Sections 3001 & 3004 and directed reductions, sequestration adjustments, reprogrammings, and the SBIR/STTR transfer offset by Congressional adds.

FY 2014: Decrease reflects congressional reductions for program growth, the section 8023 FFRDC reduction, offset by an increase to the Plan X program.

FY 2015: Decrease reflects the completion of the BOLT program in the Language Technology Project (IT-04) in addition to the ending of the Advanced Vehicle Manufacturing programs in Project IT-02 (Meta and IFab).

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency			Date: March 2014
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	85.540	72.028	39.800	-	39.800	54.598	50.746	77.406	78.746	-	-

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computer hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems. One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build large complex software systems. Powerful new approaches and tools are needed to enable the rapid and efficient production of new software, including software that can be easily changed to address new requirements and can adjust dynamically to platform and environmental perturbations. The project will ensure accessibility and usability to a wide range of application developers, not just computational science experts.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Power Efficiency Revolution For Embedded Computing Technologies (PERFECT)	27.370	38.337	33.800

Description: The Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) program will provide the technologies and techniques to overcome the power efficiency barriers which currently constrain embedded computing systems capabilities and limit the potential of future embedded systems. The warfighting problem this program will solve is the inability to process future real time data streams within real-world embedded system power constraints. This is a challenge for embedded applications, from Intelligence, Surveillance and Reconnaissance (ISR) systems on unmanned air vehicles through combat and control systems on submarines. The PERFECT program will overcome processing power efficiency limitations using near threshold voltage operation, massive and heterogeneous processing concurrency, new architecture concepts, and hardware and software approaches to address system resiliency, combined with software approaches to effectively utilize resulting system concurrency and data placement to provide the required embedded system processing power efficiency.

FY 2013 Accomplishments:
- Discovered power kernels for embedded DoD applications, including ISR and encryption capabilities.
- Established initial simulation infrastructures for evaluating temporal and power efficiency for DoD embedded subsystems.
- Developed theoretical near threshold voltage and resiliency trade-offs for power efficiency.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Identified key language extensions and approaches required for the development of massively parallel software. ***FY 2014 Plans:*** - Develop an analytical modeling framework for fundamental design trade-off analysis and documentation for local resilience and power optimizations and global optimization methodologies and techniques. - Establish algorithmic analysis and design methodologies for power efficient and resilient processing. - Define power efficient, heterogeneous, highly concurrent conceptual architectural design approaches. - Define and evaluate the impact of 3D approaches for power efficient processing. ***FY 2015 Plans:*** - Incorporate test chip results - circuit, architecture, communication, power management, 3D - for design optimization and simulation refinement for continuing architectural development efforts. - Develop compiler algorithms supporting communication- avoiding optimization, concepts for optimizing parallel codes and language-based auto-tuning. - Deliver system-level integrated analytical modeling methodology and software analysis toolset for cross-layer, energy-constrained resilience optimization, processor, memory, and energy-reliability trade-offs. - Publically release new hardware description language and modeling/simulation infrastructure incorporating the evaluation and development of algorithms, specializers, hardware architectures, and resiliency techniques.			
Title: Cortical Processor ***Description:*** Capturing complex spatial and temporal structure in high-bandwidth, noisy, ambiguous data streams to meet DoD's needs cannot be achieved even by state-of-the-art signal/image analysis systems. However, there is a processing structure in nature, the mammalian neocortex, that efficiently captures spatial and temporal structure and routinely solves the most difficult recognition problems in real-time and is a general purpose structure for a range of sensor data processing and motor control execution. The Cortical Processor program will leverage simplified models of known cortical operation to develop a new processor architecture that is optimized for running a family of algorithms known as Hierarchical Temporal Memory (HTM), providing new levels of performance and capabilities to a broad range of data recognition problems. HTM models map well to simple, massively parallel, signal processor arrays and a cortical processor leveraging advances in dense memory structures on a Complementary Metal-Oxide-Semiconductor (CMOS) chip running at a few watts can perform orders of magnitude larger tasks than an HTM system simulated by commercial efforts on large data-center clusters. With certain specialized circuits, several orders of magnitude improvement in throughput and efficiency will be possible with the cortical processor, enabling a wide range of powerful, ultra-low power, embedded applications.	-	-	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Executing large HTM models on modest-sized embedded platforms will transform the DoD's ability to convert huge quantities of data into actionable information. By augmenting tactical sensor systems on the battlefield with the new functionalities of predictive analyses and anomaly detection, this technology will have a major impact on the abilities of autonomous vehicles, robots, and UAVs. The Cortical Processor will adapt to changing environments while reducing the need for a man in-the-loop, providing entirely new capabilities that cannot be achieved with today's commercial hardware. This technology will enable more complex missions, particularly for surveillance systems and portable analytics and knowledge extraction from vision sensors and multi-model integration for the DoD and intelligence communities. Basic research for the program is budgeted in PE 0601101E, Project CCS-02. ***FY 2015 Plans:*** - Specify cortical processor system architecture and generate performance and power estimates. - Initiate design of modular HTM coprocessor/accelerator chip. - Simulate selected transition of DoD application(s) using an HTM algorithm approach demonstrating the ability to learn and adapt.			
Title: META ***Description:*** The goal of the META program is to develop novel design flows, tools, and processes to enable a significant improvement in the ability to design complex defense systems that are verified by virtual testing. The program seeks to develop a design representation from which system designs can quickly be assembled and their correctness verified with a high degree of certainty. Such a "fab-less" design approach is complemented by a foundry-style manufacturing capability, consisting of a factory capable of rapid reconfiguration between a large number of products and product variants through bitstream re-programmability, with minimal or no resultant learning curve effects. Together, the fab-less design and foundry-style manufacturing capability is anticipated to yield substantial---by a factor of five ---compression in the time to develop and field complex defense and aerospace systems. ***FY 2013 Accomplishments:*** - Developed a domain-specific component model library for the chassis and survivability subsystems of an amphibious infantry fighting vehicle (IFV) through extensive characterization of desirable and spurious interactions, dynamics, and properties of all physics domains. - Transmitted the winning design from the first Fast Adaptable Next Generation Ground (FANG) Challenge to the iFAB foundry for fabrication of an IFV drivetrain and mobility subsystem.	36.169	20.691	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Began expanded development of META tool suite to include qualitative and relational abstraction modeling, probabilistic certificate of correctness calculations, complexity metric evaluation, non-linear Partial Differential Equation (PDE) analysis and cyber design evaluation. ***FY 2014 Plans:*** - Conclude expanded development of META tool suite to include qualitative and relational abstraction modeling, probabilistic certificate of correctness calculations, complexity metric evaluation, non-linear Partial Differential Equation (PDE) analysis, and cyber design evaluation. - Conduct preliminary developmental Beta testing and integrated demonstration testing for the expanded META tool suite including expanded capability features. - Conduct META tool transition activity to commercial Product Lifecycle Management (PLM) tool suites. - Transition META software tool suite and associated technology to the Digital Manufacturing and Design Innovation Institute (DMDII) through the use of co-funded research and formal technology transition activities for industry use.			
Title: Instant Foundry Adaptive Through Bits (iFAB)	22.001	13.000	-
Description: Instant Foundry Adaptive Through Bits (iFAB), will lay the groundwork for the development of a foundry-style manufacturing capability--taking as input a verified system design--capable of rapid reconfiguration to accommodate a wide range of design variability and specifically targeted at the fabrication of military ground vehicles. The iFAB vision is to move away from wrapping a capital-intensive manufacturing facility around a single defense product, and toward the creation of a flexible, programmable, potentially distributed production capability able to accommodate a wide range of systems and system variants with extremely rapid reconfiguration timescales. The specific goals of the iFAB program are to rapidly design and configure manufacturing capabilities to support the fabrication of a wide array of infantry fighting vehicle models and variants. Once a given design is developed and verified, iFAB aims to take the formal design representation and automatically configure a digitally-programmable manufacturing facility, including the selection of participating manufacturing facilities and equipment, the sequencing of the product flow and production steps, and the generation of computer-numerically-controlled (CNC) machine instruction sets as well as human instructions and training modules. iFAB is mostly an information architecture. Only the final assembly capability needs to be co-located under a single roof in anything resembling a conventional fabrication facility; the rest of iFAB can be geographically distributed and can extend across corporate and industrial boundaries, united only by a common model architecture and certain rules of behavior and business practices. The final assembly node of the iFAB Foundry for infantry fighting vehicles (IFV) is the Joint Manufacturing and Technology Center (JMTC) at the Rock Island Arsenal (RIA). ***FY 2013 Accomplishments:*** - Conducted a preliminary design review and critical design review (CDR) for the iFAB Foundry.			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Matured and integrated foundry infrastructure tools developed under iFAB, including manufacturing feedback and process planning. - Developed foundry infrastructure tools to assess assembly processes and requirements. - Upgraded the RIA final assembly facility of the iFAB Foundry, and installed equipment for the first FANG challenge for an amphibious IFV drivetrain and mobility subsystem. - Tested process planning, manufacturing assessment and building capabilities of the distributed foundry through pre-challenges in preparation for the first FANG challenge for an IFV drivetrain and mobility subsystem. - Provided manufacturability feedback to the META design process in support of the first FANG challenge for an IFV drivetrain and mobility subsystem. - Configured the iFAB foundry to build the winning drivetrain and mobility subsystem design from the first FANG Challenge. ***FY 2014 Plans:*** - Build and test the winning drivetrain and mobility subsystem design from the first FANG Challenge. - Provide manufacturability feedback to the META design process in support of the tool validation testing. - Transition iFAB software tool suite and associated technology to the Digital Manufacturing and Design Innovation Institute (DMDII) through the co-funded research and formal technology transition activities for industry use. - Transition all physical infrastructure for the iFAB Foundry final assembly node at RIA to JMTC.			
Accomplishments/Planned Programs Subtotals	85.540	72.028	39.800

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency			Date: March 2014
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	169.595	189.238	187.925	-	187.925	200.009	204.404	204.788	206.128	-	-

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Information Assurance and Survivability project is developing the core computing and networking technologies required to protect DoD's information, information infrastructure, and mission-critical information systems. These technologies will enable DoD information systems to operate correctly and continuously even when they are attacked, and will provide cost-effective security and survivability solutions. Technologies developed under this project will benefit other projects within this program element as well as projects in the Command, Control, and Communications program element (PE 0603760E), the Network-Centric Warfare Technology program element (PE 0603766E), the Sensor Technology program element (PE 0603767E), and other projects that require secure, survivable, network-centric information systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: High Assurance Cyber Military Systems	16.064	23.117	29.000

Description: The High Assurance Cyber Military Systems program will develop and demonstrate the technologies required to secure mission-critical embedded computing systems. The DoD is making increasing use of networked computing in systems such as military vehicles, weapon systems, ground sensors, smartphones, personal digital assistants, and other communication devices. This dependence makes it critically important that the embedded operating system provides high levels of inherent assurance. This operating system must also integrate the computational, physical, and networking elements of the system while running on a processor with very limited size, weight, and power. Consequently, it can only devote a limited share of its computational resources to security while satisfying hard real-time constraints. Recent advances in program synthesis, formal verification techniques, low-level and domain-specific programming languages, and operating systems mean that fully verified operating systems for embedded devices may be within reach at reasonable costs. The program will develop, mature, and integrate these technologies to produce an embedded computing platform that provides a high level of assurance for mission-critical military applications.

FY 2013 Accomplishments:

- Performed static and dynamic baseline assessments of selected militarily relevant vehicles before any modifications were made, discovering significant vulnerabilities in all four program platforms.
- Developed initial techniques and built prototype tools to assist in the rapid creation of high-assurance embedded computing systems on a variety of vehicles, including domain-specific languages for building and configuring flight control software.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Constructed core pieces of a high-assurance embedded operating system and attack-resilient control system for two militarily relevant vehicles using developed tools and techniques. - Formally verified full functional correctness for portions of a core operating system and targeted control-systems for selected vehicles. - Demonstrated required security properties that follow from correctness, specifically, non-transitive non-interference. ***FY 2014 Plans:*** - Demonstrate compositionality, which is the ability to construct high assurance systems out of high assurance components. - Extend the core high-assurance embedded operating system with additional functionality, including automatically generated device drivers and communication protocols. - Automatically synthesize correct-by-construction control systems from high-level specifications. ***FY 2015 Plans:*** - Formally verify full functional correctness for the extended core operating system and the automatically synthesized control systems for selected vehicles. - Demonstrate required security properties that follow from correctness for the extended core operating system and the automatically synthesized control systems. - Perform static and dynamic assessments after modifications are made on the militarily-relevant vehicles to evaluate the effectiveness of the synthesis and formal methods tools.			
Title: Vetting Commodity Computing Systems for the DoD (VET) ***Description:*** The Vetting Commodity Computing Systems for the DoD (VET) program will develop tools and methods to uncover backdoors and other hidden malicious functionality in the software and firmware on commodity IT devices. The international supply chain that produces the computer workstations, routers, printers, and mobile devices on which DoD depends provides many opportunities for our adversaries to insert hidden malicious functionality. VET technologies will also enable the detection of software and firmware defects and vulnerabilities that can facilitate adversary attack. ***FY 2013 Accomplishments:*** - Defined the requirements for the three key program challenges: the discovery of likely attack scenarios, the design of program analysis tools, and the reliable execution of diagnostics on already-compromised systems. - Developed concept of operations, created example supply chain attack scenarios, presented initial program analysis approaches, and specified diagnostic tool functionality. - Identified the initial infrastructure required to support the development of a sufficient number of challenge programs containing hidden malicious functionality to support realistic evaluations. ***FY 2014 Plans:***	7.376	17.954	21.553

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Develop relevant application programming interfaces and define formal semantics for the programming languages to be analyzed. - Produce initial prototype attack scenario generation, program analysis, and diagnostic tools. - Produce initial set of challenge programs for use in a competitive evaluation. - Perform a competitive engagement between research and adversarial challenge performers to produce measurements of research progress against program metrics. ***FY 2015 Plans:*** - Improve the effectiveness of prototype tools through further competitive engagements. - Expand the set of challenge programs to explore more complex forms of malicious hidden functionality. - Conduct an integrated end-to-end software/firmware-vetting technology demonstration relevant to potential transition partners.			
Title: Mission-oriented Resilient Clouds (MRC)	23.500	21.571	16.892
Description: The Mission-oriented Resilient Clouds (MRC) program will create technologies to enable cloud computing systems to survive and operate through cyber attacks. Vulnerabilities found in current standalone and networked systems can be amplified in cloud computing environments. MRC will address this risk by creating advanced network protocols and new approaches to computing in potentially compromised distributed environments. Particular attention will be focused on adapting defenses and allocating resources dynamically in response to attacks and compromises. MRC will create new approaches to measuring trust, reaching consensus in compromised environments, and allocating resources in response to current threats and computational requirements. MRC will develop new verification and control techniques for networks embedded in clouds that must function reliably in complex adversarial environments. ***FY 2013 Accomplishments:*** - Developed new behavior-based algorithms for detecting compromised machines. - Developed and demonstrated new resource allocation algorithms that maximize mission-effectiveness by allocating bandwidth and computing resources to higher priority tasks while avoiding the use of potentially compromised resources. - Validated the performance of new algorithms and protocols for high-assurance computing and data analysis in cloud computing systems. - Demonstrated a fault tolerant cloud computing environment that produces correct results when individual computing and network elements have been compromised or disabled. - Developed protocols for cloud monitoring and control that are tolerant of disruptions and intrusions, and validated performance on a commercial cloud.			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Began first experiment to transition automated, distributed resource allocation algorithms to United States Pacific Command (USPACOM). ***FY 2014 Plans:*** - Produce a cloud task allocation system that maximizes mission effectiveness by employing redundancy in the context of current system loads without significantly increasing hardware costs. - Implement a trustworthy programmable switch controller. - Demonstrate dynamic adaptation of data replication in response to estimated and predicted attack levels. - Implement self-healing functionality for cloud applications. - Begin evaluating technologies in Defense Information Systems Agency (DISA) testbeds to facilitate transitions into DoD clouds. - Transition research product into USPACOM distributed computing environments. ***FY 2015 Plans:*** - Demonstrate automated construction of diverse, redundant network flow paths that maximize communication resilience in clouds. - Extend consensus protocols to work between diverse, virtualized clouds and measure improvements in mission resilience. - Produce and validate a network abuse detection and mitigation system that operates in software defined networks. - Develop and demonstrate hardened services through fine-grained memory access controls that determine what valid memory addresses are read or written to by each instruction in a program. - Complete transition of one or more technologies into operational use by DISA and USPACOM.			
Title: Active Cyber Defense (ACD) ***Description:*** The Active Cyber Defense (ACD) program will enable DoD cyber operators to fully leverage our inherent home field advantage when defending the DoD cyber battlespace. In the cyber environment, defenders have detailed knowledge of, and unlimited access to, the system resources that attackers wish to gain. The ACD program will exploit emerging technologies to facilitate the conduct of defensive operations that involve immediate and direct engagement between DoD cyber operators and sophisticated cyber adversaries. Through these active engagements, DoD cyber defenders will be able to more readily disrupt, counter, and neutralize adversary cyber tradecraft in real time. Moreover, ACD-facilitated operations should cause adversaries to be more cautious and should increase their work factor by limiting the success from their efforts. ***FY 2013 Accomplishments:*** - Developed initial system requirements and concept of operations. - Drafted test plans and test scenarios for prototype assessments and identified key technical metrics for evaluation. - Held coordination meetings with potential transition partners including NSA, U.S. Cyber Command, and others. ***FY 2014 Plans:***	5.300	12.500	16.328

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Develop techniques for countering adversary cyber tradecraft and implement in early prototype software applications. - Develop detailed system designs and design documentation. - Finalize test plans and perform initial evaluations of active cyber defense prototypes in exercises with transition partners. ***FY 2015 Plans:*** - Integrate technologies into complete prototypes and demonstrate capabilities to transition partners. - Perform final test and evaluation of integrated capabilities and obtain approval for operational deployment. - Support initial operational fielding of capability.			
Title: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)	28.502	27.536	16.600
Description: The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program will develop cyber security technologies using the mechanisms of biological systems as inspiration for radically re-thinking basic hardware and system designs. Higher level organisms have two distinct immune systems: the innate system is fast and deadly but is only effective against a fixed set of pathogens; the adaptive system is slower, but can learn to recognize novel pathogens. Similarly, CRASH will develop mechanisms at the hardware and operating system level that eliminate known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH will also develop software techniques that allow a computer system to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH will develop techniques that make each computer system appear unique to the attacker and allow each system to change over time. ***FY 2013 Accomplishments:*** - Implemented a compiler that automatically produces diverse instantiations of a complete Linux operating system and demonstrated that the resulting operating system is resistant to standard attacks. - Demonstrated a novel form of moving target defense that employs several automatically constructed diverse implementations of the same algorithm. - Produced a tool that finds and fixes bugs and attendant security vulnerabilities in operating system and utility software. - Demonstrated roll-back and recovery on two production-scale applications with substantially reduced requirements for human involvement. - Developed technology to mitigate vulnerabilities found in widely used embedded systems such as telephones and printers and initiated efforts to transition the technology into commercial use. ***FY 2014 Plans:*** - Complete the implementation of two novel secure processors and operating systems and demonstrate the ability to resist all attacks mounted by a red-team. - Demonstrate the capability to wrap C2 software codes as a means to thwart cyber attack.			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Demonstrate real-time, continuous validation of system compliance with security specifications. - Demonstrate the ability of two or more complete systems to block, survive, and recover from multiple attacks and automatically repair vulnerabilities. - Transition research products into one or more embedded systems and a secure router for military use. ***FY 2015 Plans:*** - Automatically produce diverse instantiations of one or more complete operating systems. - Deliver a web server that enables creation of secure web sites from untrusted code. - Deliver a web server and browser that enable creation of secure web applications from untrusted code. - Demonstrate policy-based application monitoring and hardware-assisted self-healing of multiple applications.			
Title: Rapid Software Development using Binary Components (RAPID) ***Description:*** The Rapid Software Development using Binary Components (RAPID) program will develop a system to identify and extract software components for reuse in new applications. The DoD has critical applications that must be ported to future operating systems. In many cases, the application source code is no longer available requiring these applications to continue to run on insecure and outdated operating systems, impacting operations. Advanced technology research for the program is budgeted in PE 0603760E, Project CCC-04. ***FY 2013 Accomplishments:*** - Developed an initial low level virtual machine translation engine. - Completed the initial implementation of the user interface. ***FY 2014 Plans:*** - Fully integrate technologies into a single architecture and standardize interfaces to enable partners to interoperate with the system. - Develop a single user interface that combines technical area views and supports mobile operation. ***FY 2015 Plans:*** - Develop new software component reuse capabilities to optimize application performance in realistic scenarios and enable an expanded concept of operations. - Implement new capabilities in modules designed to interoperate seamlessly with deployed RAPID prototype systems. - Integrate new modules into prototype RAPID systems deployed at transition partner sites and support initial operations.	2.049	8.198	13.396
Title: Anomaly Detection at Multiple Scales (ADAMS) ***Description:*** The Anomaly Detection at Multiple Scales (ADAMS) program will develop and apply algorithms for detecting anomalous, threat-related behavior of systems, individuals, and groups over hours, days, months, and years. ADAMS will	15.000	17.612	9.750

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
develop flexible, scalable, and highly interactive approaches to extracting actionable information from information system log files, sensors, and other instrumentation. ADAMS will integrate these anomaly detection algorithms to produce adaptable systems for timely insider threat detection. ***FY 2013 Accomplishments:*** - Refined and created techniques for detecting malicious insiders, delineated assumptions/conditions under which they are valid/ invalid, and specified their effective combination. - Created a comprehensive library of test data and quantified probabilities of detection and false alarm for anomalous non-threat and threat behaviors. - Developed technologies to manage the number of anomalies, focus computing resources on ambiguous results, and prioritize threats. - Demonstrated the capability to identify anomalous behavior suggestive of a threat in real time on streaming data. ***FY 2014 Plans:*** - Develop and implement technology to capture analyst expertise for assessing and explaining detected anomalies and incorporate such user feedback in decision loops for counter intelligence (CI) agents without highly specialized computer science knowledge. - Create the capability to incorporate direct CI agent feedback to improve coverage of threat types. - Develop and implement technology that is adaptable to a wide variety of organizational structures, workflows, and data sources. - Develop techniques to provide the evidence needed to initiate focused response activities. ***FY 2015 Plans:*** - Develop an integrated prototype anomaly/threat detection system suitable for rapid deployment in an operational environment. - Harden prototype and obtain DoD Information Assurance Certification and Accreditation Process approval for use on military networks. - Conduct and evaluate initial prototype in a large scale environment with operational partners.			
Title: Active Authentication* ***Description:*** *Previously funded in PE 0601101E, Project CYS-01. The Active Authentication program will develop more effective user identification and authentication technologies. Current authentication approaches are typically based on long, complex passwords and incorporate no mechanism to verify the user originally authenticated is the user still in control of the session. The Active Authentication program will address these issues by focusing on the unique aspects of the individual (i.e., the cognitive fingerprint) through the use of software-based biometrics that	6.489	13.100	8.025

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
continuously validate the identity of the user. Active Authentication will integrate multiple biometric modalities to create a system that is accurate, robust, and transparent to the user. ***FY 2013 Accomplishments:*** - Developed open application programming interfaces to allow the ready integration of third-party software and hardware biometrics. - Initiated development of an additional authentication platform suitable for deployment on DoD hardware. - Implemented multiple advanced authentication mechanisms in prototype systems potentially suitable for use on DoD networks. - Coordinated with U.S. Army Intelligence and Information Warfare Directorate for transition into Army biometric-enabled authentication platform. ***FY 2014 Plans:*** - Demonstrate enhanced authentication using multiple biometrics representing complementary aspects of the individual. - Evaluate the level of confidence that is achievable using multiple advanced authentication mechanisms and quantify the resulting level of security using red teaming and other techniques. - Prototype an authentication platform suitable for DoD use in collaboration with potential transition sponsors. - Initiate development of multiple authentication biometrics suitable for deployment on mobile hardware for potential use by the DoD. ***FY 2015 Plans:*** - Demonstrate multiple authentication biometrics suitable for deployment on mobile hardware for potential use by the DoD. - Prove flexibility of underlying prototype platform by creating an additional authentication platform suitable for DoD. - Prototype an authentication platform suitable for use on mobile hardware in collaboration with potential transition sponsors.			
Title: Integrated Cyber Analysis System (ICAS) ***Description:*** The Integrated Cyber Analysis System (ICAS) program will develop techniques to automatically discover probes, intrusions, and persistent attacks on enterprise networks. At present, discovering the actions of capable adversaries requires painstaking forensic analysis of numerous system logs by highly skilled security analysts and system administrators. ICAS will develop technologies to allow for the correlation of interactions and behavior patterns across all system data sources and thereby rapidly uncover aberrant events and detect system compromise. This includes technologies for automatically representing, indexing, and reasoning over diverse, distributed, security-related data and system files. ***FY 2013 Accomplishments:*** - Developed an approach for transforming log/system file formats into a unified schema as the basis for an actionable view of enterprise operational security.	3.044	10.000	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Conceptualized indexing schemes specialized to system files/security data and suitable for use across federated enterprise architectures. - Identified potential transition partners within DoD and established operational requirements. ***FY 2014 Plans:*** - Develop and implement algorithms for automatically identifying and quantifying specific security risks on enterprise networks. - Conduct initial technology demonstrations including automatic indexing of data sources, common language integration, and reasoning across federated databases. - Complete alpha versions of applications which meet all program objectives and test in coordination with transition partners. - Integrate, evaluate, and optimize algorithms via testing against attacks/persistent threats provided by transition partners. ***FY 2015 Plans:*** - Complete fully functional beta versions of the applications with operational stability suitable for testing at transition partner locations. - Harden and deploy solutions to transition partner networks throughout the DoD.			
Title: Safer Warfighter Computing (SAFER) ***Description:*** The Safer Warfighter Computing (SAFER) program is creating a technology base for assured and trustworthy Internet communications and computation, particularly in untrustworthy and adversarial environments. SAFER creates automated processes and technologies to enable military users to send and receive content on the Internet, utilizing commercially available hardware and software, in ways that avoid efforts to deny, locate, or corrupt communications. SAFER is also developing technology for performing computations on encrypted data without decrypting it first through fully homomorphic encryption and interactive, secure multi-party computation schemes. This will enable, for example, the capability to encrypt queries and compute an encrypted search result without decrypting the query. This technology will advance the capability to run programs on untrusted hardware while keeping programs, data, and results encrypted and confidential. This mitigates the important aspect of supply chain compromise. ***FY 2013 Accomplishments:*** - Performed independent, adversarial assessment of the effectiveness of technologies to prevent communication localization and detection. - Demonstrated two developmental technologies for anonymous web communications which are much more difficult for an adversary to detect or block. - Demonstrated an initial field programmable gate array implementation of fully homomorphic encryption offering an order of magnitude performance improvement over optimized software implementations.	17.680	15.150	4.066

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Performed independent benchmarks of fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation. - Demonstrated two orders of magnitude improvement in performance of fully homomorphic encryption. ***FY 2014 Plans:*** - Integrate decoy routing, parallelized group messaging, dynamic traffic camouflage, and rendezvous strategy technologies into common internet browsing applications. - Conduct the final independent, adversarial assessment of the effectiveness of technologies to prevent communication localization and detection, including newly developed adversarial techniques. - Reduce ciphertext expansion while improving software performance in fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation, and perform independent benchmarks. - Demonstrate an additional two orders of magnitude improvement in the performance of fully homomorphic encryption. - Refine field programmable gate array implementation of fully homomorphic encryption to yield a further order of magnitude performance improvement over optimized software implementation. ***FY 2015 Plans:*** - Demonstrate safe, anonymous internet communications applications such as web access, Voice over Internet Protocol (VOIP), and streaming video, at scale. - Further optimize field programmable gate array and software implementations of fully homomorphic encryption to double performance over prior implementations.			
Title: Logan ***Description:*** The Logan program will provide DoD enhanced capabilities to conduct Computer Network Attack (CNA). Techniques will be developed to disrupt and degrade adversary information systems and network operations, with particular interest in techniques likely to be robust to adversary countermeasure strategies. ***FY 2013 Accomplishments:*** - Formulated CNA techniques and implemented these in initial software routines. - Developed manual prototypes for operational transition. ***FY 2014 Plans:*** - Automate and test prototypes in conjunction with transition partner. - Optimize and harden prototypes and complete transition. ***FY 2015 Plans:***	6.000	9.803	4.697

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Transition automated system for operational implementation.			
Title: Integrity and Reliability of Integrated CircuitS (IRIS)	18.500	1.000	-

Description: Integrated circuits (ICs) are core components of most electronic systems developed for the Department of Defense. However, the DoD consumes a very small percentage of the total IC production in the world. As a result of the globalization of the IC marketplace, much of the advanced IC production has moved to offshore foundries, and these parts make up the majority of ICs used in today's military systems.

Without the ability to influence and regulate the off-shore fabrication of ICs, there is a risk that parts acquired for DoD systems may not meet stated specifications for performance and reliability. This risk increases considerably with the proliferation of counterfeit ICs in the marketplace, as well as the potential for the introduction of malicious circuits into a design.

The Integrity and Reliability of Integrated CircuitS (IRIS) program seeks to develop techniques that will provide electronic system developers the ability to validate the function of digital, analog and mixed-signal ICs non-destructively, given limited data about the chip's detailed design specifications. These techniques will include advanced imaging for identification of functional elements in deep sub-micrometer Complementary Metal-Oxide Semiconductor (CMOS) circuits, as well as computational methods to deal with the extremely difficult problem of determining device connectivity.

Finally, the IRIS program will develop innovative methods to determine the reliability of an IC by testing a limited number of samples. The current understanding of IC aging mechanisms, including negative bias temperature instability (NBTI), hot carrier injection (HCI), time-dependent dielectric breakdown (TDDB) and electromigration (EM) will be leveraged to develop unique diagnostic test techniques.

FY 2013 Accomplishments:
- Demonstrated the ability to identify design primitives (transistors, capacitors, resistors), memory elements and interconnects through non-destructive imaging, and derived a net-list from these components.
- Demonstrated functional derivation of modified digital and mixed-signal ICs at the 45 nm CMOS node.
- Demonstrated reliability derivation from reduced sample sizes of modified ICs.
- Demonstrated non-destructive techniques for functional analysis of a digital IC.
- Demonstrated tools for functional derivation from third-party IP (Intellectual Property) blocks for both Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs).
- Developed digital and mixed-signal test articles appropriate for testing techniques for identifying unintended circuits and circuit functions.

FY 2014 Plans:

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Exercise completed methods for non-destructive imaging, circuit extraction and functional derivation. - Demonstrate methods for reliability analysis for improved accuracy, functionality and efficacy.			
Title: Supply Chain Hardware Intercepts for Electronics Defense (SHIELD)	-	5.000	16.500
Description: Counterfeit electronic parts are becoming ubiquitous, and pose a threat to the integrity and reliability of DoD systems. Detection of counterfeit components by current means is expensive, time-consuming, and of limited effectiveness. Maintaining complete control of the supply chain using administrative controls incurs substantial costs and has limitations. Current methods of detection involve a wide variety of techniques ranging from functional testing to physical inspections which may still miss certain classes of counterfeits. There have also been attempts by the semiconductor market to protect electronic components through the use of technology embedded in the component or its packaging. However, most methods are specific to a manufacturer's component and as such address only those issues deemed critical to that manufacturer. Some methods can be circumvented, or require slow, expensive, off-site forensic analysis to verify authenticity. The Supply Chain Hardware Intercepts for Electronics Defense (SHIELD) program, leveraging and expanding on previous activities in the IRIS program, will develop a technology capable of confirming, at any time, the authenticity of once-trusted parts, even after they have transited a complex global supply chain. SHIELD will prevent counterfeit component substitution by incorporating a small, inexpensive additional silicon chip ("dielet") within the Integrated Circuit (IC) package. The dielet will provide a unique and non-clonable ID as well as anti-tamper features. The microscopic-size dielet embedded in the electronic component packaging will be inductively powered and scanned by an authentication induction coil brought into very close proximity to the packaged chip, thus allowing for verification of chip identity. ***FY 2014 Plans:*** - Develop behavioral models for SHIELD performance and power consumption. - Establish server communication protocols, encryption standards, network architectures. - Design test sites for technology, surrogate dielet structures for package tests. - Define process modifications needed to accommodate SHIELD insertions. ***FY 2015 Plans:*** - Develop technologies to allow secure key and ID storage and prevent tampering with the dielet. - Design a compact encryption engine that enables a very small, low power, and low-cost dielet. - Define a power and communication inductive coil protocol. - Simulate and prototype dielet package-insertion techniques for placing SHIELD on product.			
Title: Protecting Cyber Physical Systems (PCPS)	-	-	9.525

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Description: The Protecting Cyber Physical Systems (PCPS) program will create new technologies for ensuring the availability and integrity of cyber physical systems. The near-ubiquitous use of embedded computing in commercial, industrial, and medical devices, the emergence of software defined networking, and the importance of automatic control to U.S. civilian and military critical infrastructure make this a national security issue. PCPS will develop technologies to monitor heterogeneous distributed industrial control system networks, detect anomalies that require rapid assessment, and mitigate sensor spoofing and denial of service attacks. Mechanisms to ensure the integrity of remote firmware updates and mitigate attacks for which wireless interfaces provide a vector will also be developed. PCPS technologies will transition to military installations and commercial industry. ***FY 2015 Plans:*** - Develop technologies to monitor heterogeneous distributed industrial control system networks, detect anomalies that require rapid assessment, and mitigate sensor spoofing and denial of service attacks. - Create mechanisms to ensure the integrity of remote firmware updates. - Develop approaches for mitigating the risks associated with wireless interfaces.			
Title: Active-Reactive Cyber Systems (ARCS)	-	-	8.500
Description: The Active-Reactive Cyber Systems (ARCS) program will develop technologies to enable hosts, systems, and networks to actively sense for threats and to dynamically react to attacks. Current cyber defense technologies are statically configured to satisfy a complex set of engineering trade-offs and are rarely optimized for the dynamic environments in which they are deployed. ARCS technologies will use organic sensors, remote instrumentation, and other sources of cyber situation awareness information to continuously optimize cyber defenses. Host and network management and control technologies will be developed that enable systems to fight through cyber attack and provide essential mission services by repurposing resources to critical services, repairing damaged resources, and utilizing degraded resources. ARCS software agents will protect data stores by implementing dynamic access controls that consider user and program authorization within the context of the cyber situation and network defense posture. ***FY 2015 Plans:*** - Develop techniques that use organic sensors, remote instrumentation, and other sources of cyber situation awareness information to continuously optimize cyber defenses. - Develop host and network management and control technologies that enable systems to fight through cyber attack and provide essential mission services. - Develop software agents that implement dynamic access controls that consider user and program authorization within the context of the cyber situation and network defense posture.			
Title: Adaptable Information Access and Control (AIAC)	-	-	7.093

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Description: The Adaptable Information Access and Control (AIAC) program will create the capability to dynamically, flexibly, and securely share highly selective information across enterprise boundaries. In the civilian sphere, there is a recognized need for technologies that limit the sharing of information between commercial entities and U.S. government agencies to the greatest extent possible consistent with national security requirements. Similarly, the U.S. military is increasingly involved in humanitarian operations that require highly selective sharing of data with a heterogeneous mix of allies, coalition partners, and other stakeholders. AIAC will create confidentiality, privacy, multi-level security, discretionary access control, and policy engine technologies to allow tailored access to a specific datum but not an entire database/file system/corpus. AIAC is timely due to recent progress on cryptographic techniques such as homomorphic encryption and secure multiparty computation. Additional technologies that will be developed and incorporated include automated policy-driven releasability assessment and redaction, tactical obfuscation, and time-limited-access controls. The program will address the diverse and stringent legal and ethical requirements related to security, privacy, authentication, authorization, auditing, monitoring, access, and control encountered in both civilian and military environments. To facilitate deployment, AIAC technologies will be designed to work with the virtualization, cloud computing, and software-defined networking technologies now widely used in both civilian and military environments. ***FY 2015 Plans:*** - Formulate access control schemes appropriate for diverse civilian, intelligence, law enforcement, and coalition use cases with particular focus on privacy-preserving analytics. - Architect an access control policy engine for seamless interoperability with common computing and networking infrastructure software. - Create technologies for confidentiality, privacy, multi-level security, discretionary access controls, automated policy-driven releasability assessment and redaction, tactical obfuscation, computing on encrypted data, and time-limited-access controls.			
Title: Cyber Genome ***Description:*** The Cyber Genome program develops techniques to automatically characterize, analyze, and identify malicious code and determine the evolutionary relationship between new never-before-seen malware samples and older known malware. This enables the automatic detection of future malware variants. Such automation is critically important because the global production of malware is growing explosively and threatens to overwhelm current labor-intensive practices. Cyber Genome also develops advanced capabilities to enable positive identification of malicious code substructures and functionality. ***FY 2013 Accomplishments:*** - Developed techniques to automatically and reliably extract forensically-meaningful traits such as authorship, compiler, toolkit, and obfuscation techniques. - Enhanced co-clustering and binary analysis techniques to enable the automatic identification of re-used components.	15.949	6.697	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Developed operationally relevant use case test scenarios with transition partners and conducted initial use case validation tests. - Implemented prototypes and evaluated their effectiveness on realistic malware samples. - Executed an MoA with the FBI to evaluate the performance of the automated malware analysis tools on operational data. ***FY 2014 Plans:*** - Demonstrate significant improvement to provenance determination through the use of the automatically extracted traits. - Demonstrate final prototypes capable of detecting a single interesting targeted threat from a stream of at least 10K uninteresting mass-infection malware samples. - Evaluate the effectiveness of prototype systems in conjunction with transition sponsors and complete transition.			
Title: Cyber Fast Track ***Description:*** The Cyber Fast Track program created more flexible, responsive methods for securing computing systems that operate in challenging environments and reduced security risk without requiring lengthy development cycles. Under Cyber Fast Track, small agile teams worked under rapid development cycles to create cyber security applications. ***FY 2013 Accomplishments:*** - Expanded outreach to customers/transition sponsors. - Completed efforts and transitioned technologies to multiple DoD agencies.	4.142	-	-
Accomplishments/Planned Programs Subtotals	169.595	189.238	187.925

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency			Date: March 2014
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-04 / *LANGUAGE TECHNOLOGY*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
IT-04: *LANGUAGE TECHNOLOGY*	-	59.650	70.482	39.333	-	39.333	50.223	81.539	57.199	74.539	-	-

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Language Technology project is developing powerful new technologies for processing foreign languages that will provide critical capabilities for a wide range of military and national security needs. The technologies and systems developed in this project will enable our military to automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means. Current U.S. military operations involve close contact with a wide range of cultures and peoples. Warfighters need speech-to-speech translation systems that enable communication with local populations, especially two-way (foreign-language-to-English and English-to-foreign-language) translation. In addition, foreign-language news broadcasts, web-posted content, and captured foreign-language hard-copy documents can provide insights regarding local and regional events, attitudes, and activities. Language translation, information extraction, and other language analytic systems contribute to the development of critical intelligence and situational awareness. Technologies for translation of informal genres (online discussion groups, messaging, and telephone conversation) of voice and text, as well as capabilities to automatically collate, filter, synthesize, summarize, and present relevant information in near real-time will enhance situational awareness.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Broad Operational Language Translation (BOLT)	40.206	45.113	-
Description: The Broad Operational Language Translation (BOLT) program is enabling communication in informal and dialectal genres. Historically, foreign language translation technology was geared toward formal content, like broadcast media and newswire, but did not address informal or dialectal genres. BOLT is developing new approaches to automated language translation, human-machine multimodal dialogue, and language generation and applying these to informal genre such as online discussion groups, messaging, and telephone conversation. BOLT will leverage the strengths of statistical and rule-based approaches to form hybrid machine translation techniques that are more robust to linguistic dialectal variation; develop new techniques for modeling word relationships, functions, and context; and utilize syntactic and semantic patterns to fill in the linguistic gaps inherent in conversational language and to accelerate statistical learning. While Chinese and dialectal Arabic are the two languages addressed directly in BOLT, techniques developed for these two languages will have wide applicability to other languages and dialects. BOLT will enable warfighters and military/government personnel to readily communicate with coalition partners and local populations and will enhance intelligence through better exploitation of all language sources.			
FY 2013 Accomplishments: - Developed new and improved algorithms for translating two informal genres of Arabic and Chinese text, online discussion groups and messaging, and created annotated corpora for training and testing the algorithms.			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Developed methods for Egyptian dialectal Arabic that are applicable to all Egyptian Arabic informal genres and used these to develop databases, tools, and algorithms to translate Tunisian dialectal Arabic. - Developed algorithms for automatically assessing the degree of confidence in both the automatic speech recognition and machine translation hypotheses in a human-human dialogue system and specialized these to Arabic-English dialogue. - Developed enhanced automatic Arabic speech recognition techniques capable of handling garbled and ambiguous speech and words outside the vocabulary of the machine and integrated these into a robust bi-directional Arabic-English dialogue system. ***FY 2014 Plans:*** - Develop improved algorithms for translating two informal genres of Arabic and Chinese text, online discussion groups and messaging, to enable comprehension of colloquialisms and idiomatic speech and add a third genre, telephone conversation. - Use methods developed for Egyptian and Tunisian dialectal Arabic to create databases, tools, and algorithms for additional Arabic dialects. - Enhance bi-directional Arabic-English dialogue systems by incorporating topic modeling and exploiting cross-utterance context recognition. - Develop dialogue management techniques such as computer-moderated turn-taking to avoid divergence as an approach for improving the performance of bi-directional Arabic-English dialogue systems. - Complete the annotated corpora of Arabic and Chinese informal genre data by adding new dialects and enhance their utility by incorporating additional annotations. - Generalize Arabic dialectal databases, tools, and algorithms to make it straightforward to add Arabic dialects. - Work with transition partners to identify insertion opportunities and transition algorithms for translating informal genres of Arabic and Chinese.			
Title: Deep Exploration and Filtering of Text (DEFT) ***Description:*** The Deep Exploration and Filtering of Text (DEFT) program will enable automated extraction, processing, and inference of information from text in operationally relevant application domains. A key DEFT emphasis is to determine the implied and hidden meaning in text through probabilistic inference, anomaly detection, and disfluency analysis. To accomplish this, DEFT will develop and apply formal representations for basic facts, spatial, temporal, and associative relationships, causal and process knowledge, textually entailed information, and derived relationships and correlated actions/events. DEFT inputs may be in English or in a foreign language and sources may be completely free-text or semi-structured reports, messages, documents, or databases. DEFT will extract knowledge at scale for open source intelligence and threat analysis. Planned transition partners include the intelligence community and operational commands. ***FY 2013 Accomplishments:*** - Developed initial methods and algorithms to derive meaning from context for words that may have implicit or hidden meanings and to extract and disambiguate events in a document or set of documents.	15.946	25.369	28.333

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Implemented preliminary algorithms that use domain knowledge to infer implicit information from multiple facts and statements, answer questions, and generate hypotheses in domains of military interest. - Developed training data sets and queries for science and technology, human-behavioral-social-cultural, and asymmetric threat domains and performed evaluation experiments. - Designed new workflows in collaboration with end-users to enhance operational efficiency and effectiveness. ***FY 2014 Plans:*** - Develop methods and algorithms for reasoning about both explicitly and implicitly expressed opinions and beliefs, for extracting causal knowledge, and for finding hidden meaning based on anomalous usages and disfluencies in a document or set of documents. - Conduct performance evaluations on data sets related to event representation, anomaly detection, and inference. - Expand capabilities to additional application problems and domains in collaboration with end-users. - Demonstrate feasibility of deep extraction and filtering for selected end-user applications and transition initial sets of algorithms to end-users for enhanced workflows. ***FY 2015 Plans:*** - Develop technology for extracting belief, sentiment, and intent; for representing geo-spatial features and temporal events; and for inference, summarization, and alerting from a set of documents. - Integrate multiple complementary algorithms into a comprehensive and consistent functional suite to support end-user workflows and problems. - Transition algorithm suites and conduct effectiveness assessments at end-user sites.			
Title: Foreign Language Rapid Response (FLRR) ***Description:*** The Foreign Language Rapid Response (FLRR) program will develop the capability to rapidly construct human language technologies for foreign languages. Historically, exploiting foreign language materials required protracted effort and as a result systems exist only for languages in widespread use and in high demand. The military operates globally and frequently encounters less common low-resource languages for which no automated human language technology capability exists. FLRR technologies will identify the commonalities between a newly-encountered low-resource language and high-resource languages and will identify language universals to rapidly re-purpose existing language technologies to the low-resource language. This will enable the rapid creation of automated language technology systems for cross-language intelligence and strategic communications. ***FY 2015 Plans:*** - Identify the universal properties of language to serve as the basis for an extensible family of human language technologies. - Develop techniques for quantifying the linguistic similarity of language usage in diverse documents and media.	-	-	11.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Develop semantic techniques for identifying the common topics, themes, and sentiment in a collection of snippets in diverse foreign languages. - Create a baseline toolkit to rapidly develop initial document triage capability for a new low-resource language document collection. - Develop techniques for learning language from conversation about the things and people in the immediate environment.			
Title: Robust Automatic Translation of Speech (RATS) ***Description:*** The Robust Automatic Transcription of Speech (RATS) program addressed conditions in which speech signals are degraded by distortion, reverberation, and/or competing conversation. Robust speech processing technologies enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite a noisy or reverberant environment. RATS technology isolated and delivered pertinent information to the warfighter by detecting periods of speech activity and discarding silent portions, determining the language spoken, identifying the speaker, and recognizing key words in challenging environments. ***FY 2013 Accomplishments:*** - Developed and implemented effective processing techniques for noisy environments, including speech activity detection, language identification, speaker identification, and keyword spotting. - Evaluated performance showing substantial progress on noisy and degraded speech signals from the program-generated data corpus. - Conducted tests of training systems on field-collected data and tested systems in realistic environments. - Established a relationship with Offutt AFB to obtain real data and perform testing on site at the user location.	1.998	-	-
Title: Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) ***Description:*** The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program developed and integrated technology to enable exploitation of foreign language, hand-written documents. This technology is crucial to the warfighter, as documents including notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images captured in the field may contain extremely important time-sensitive information. The MADCAT program addressed this need by producing devices to convert such captured documents from Arabic into readable English in the field. MADCAT substantially improved applicable technologies, in particular document analysis and optical character recognition/ optical handwriting recognition. MADCAT integrated these improved technologies with translation technology and created prototypes for field trials. ***FY 2013 Accomplishments:*** - Transitioned tightly integrated technology prototypes to military and intelligence operations centers. - Trained and tested techniques on field-collected data.	1.500	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Improved MADCAT technologies transcribing and translating field-collected handwritten, machine-printed, and mixed handwritten and machine-printed documents.			
Accomplishments/Planned Programs Subtotals	59.650	70.482	39.333

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency			Date: March 2014
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-05 / *CYBER TECHNOLOGY*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
IT-05: *CYBER TECHNOLOGY*	-	33.745	67.849	67.349	-	67.349	35.014	-	-	-	-	-

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Cyber Technology project develops technology to increase the security of military information systems and the effectiveness of cyber operations. Over the past decade the DoD has embraced net-centric warfare by integrating people, platforms, weapons, sensors, and decision aids. Adversaries seek to limit this force multiplier through cyber attacks intended to degrade, disrupt, or deny military computing, communications, and networking systems. Technologies developed under the Cyber Technology project will ensure DoD net-centric capabilities survive adversary cyber attacks and will enable new cyber-warfighting capabilities. Promising technologies will transition to system-level projects.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Plan X	20.796	37.919	41.619

Description: The Plan X program will develop technologies to enable comprehensive awareness and understanding of the cyber battlespace as required for visualizing, planning, and executing military cyber warfare operations. This includes intelligence preparation of the cyber battlespace, indications and warning of adversary cyber actions, detection of cyber-attack onset, cyber-attacker identification, and cyber battle damage assessment. Plan X will create new graphical interfaces that enable intuitive visualization of events on hosts and networks to aid in the planning and execution of cyber warfare. Plan X will extend operationally meaningful measures to project quantitatively the collateral damage of executed cyber warfare missions.

FY 2013 Accomplishments:
- Mapped network topologies consisting of thousands of nodes derived from millions of traceroute outputs.
- Generated and validated cyber mission plans at operationally relevant scales and speeds.
- Created a cyber domain specific language with binding to existing operational tools and cyber warfare mission planning interface.
- Built initial range infrastructure supporting hundreds of nodes in a dynamic topology.

FY 2014 Plans:
- Release Plan X 1.0, including product launch and developer workshop.
- Coordinate development with operators from Air Force, Navy, Marine Corps, and Army cyber components and U.S. Cyber Command.
- Develop commander, planner, and operator views for the user interface.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-05 / *CYBER TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Create automated network simulation technology to model the cyber battlespace, generate cyber warfare mission plans, and script cyber warfare missions using domain specific languages. ***FY 2015 Plans:*** - Create runtime environment and platforms capable of automatically deploying cyber warfare mission scripts. - Release Plan X 2.0, including product launch and developer workshop. - Demonstrate cyber battle damage assessment. - Demonstrate capabilities by developing complex cyber training missions and employ system in a large-scale exercise (e.g., Cyber Flag).			
Title: Crowd Sourced Formal Verification (CSFV) ***Description:*** The Crowd-Sourced Formal Verification (CSFV) program will create technologies that enable crowd-sourced approaches to securing software systems through formal verification. Formal software verification is a rigorous method for proving that software has specified properties, but formal verification does not currently scale to the size of software found in modern weapon systems. CSFV will enable non-specialists to participate productively in the formal verification process by transforming formal verification problems into user-driven simulations that are intuitively understandable. ***FY 2013 Accomplishments:*** - Developed approaches for mapping high-level formal software verification problems into user-driven simulations. - Developed techniques for inferring specification and coding errors from the solutions to these simulations and for automatically generating the appropriate annotations to aid formal verification. - Developed web-based infrastructure to support large scale formal software verification workflows. - Developed and tested the concept on a moderately-sized computer program consisting of thousands of lines of source code. ***FY 2014 Plans:*** - Develop five web-based interactive computer simulations based on mapped high-level software specifications and codes. - Launch and maintain public web site to attract the widest possible base for crowd-sourcing formal verifications. - Apply simulations to large Java and C computer programs consisting of hundreds of thousands of lines of source code. - Map solutions as code annotations back into formal verification tools and assess the effectiveness of these solutions by verifying the absence of errors on the MITRE Common Weakness Enumeration/SANS Institute Top 25 lists. - Refine initial simulations and develop new simulations for greater verification effectiveness. ***FY 2015 Plans:*** - Refine simulations to make them accessible to a large set of non-specialists. - Augment simulations to handle very large Java and C computer programs consisting of millions of lines of source code. - Enhance public web site to include these new simulations.	12.949	14.680	8.898

Exhibit R-2A, RDT&E Project Justification: PB 2015 Defense Advanced Research Projects Agency		Date: March 2014
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-05 / *CYBER TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
- Assess effectiveness of the new simulations on the large-sized code targets.			
Title: Cyber Grand Challenge (CGC)* ***Description:*** *Formerly Cyber Warfare Control System (CWCS) The Cyber Grand Challenge (CGC) program will create automated defenses that can identify and respond to cyber attacks more rapidly than human operators. CGC technology will monitor defended software and networks during operations, reason about flawed software, formulate effective defenses, and deploy defenses automatically. Technologies to be developed and integrated may include anomaly detection, Monte Carlo input generation, case-based reasoning, heuristics, game theory, and stochastic optimization. The CGC capability is needed because highly-scripted, distributed cyber attacks exhibit speed, complexity, and scale that exceed the capability of human cyber defenders to respond in a timely manner. DARPA will incentivize competition through a Grand Challenge in which CGC technologies compete head-to-head. ***FY 2014 Plans:*** - Develop instrumented competition framework for automated cyber defense. - Initiate development of automated cyber defenders to identify flaws and formulate defenses. - Conduct competitive assessments to identify the most promising technology solutions. ***FY 2015 Plans:*** - Extend development of automated cyber defenders to allow real time in situ network defense decision making. - Develop a cyber research corpus using techniques from game theory, other quantitative disciplines, and emergent behavior. - Conduct mid-term evaluation of cyber technologies through competitive challenges.	-	15.250	16.832
Accomplishments/Planned Programs Subtotals	33.745	67.849	67.349

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.