Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Defense Advanced Research Projects Agency	Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
Total Program Element	-	315.923	341.358	353.635	-	353.635	353.925	359.959	344.530	354.091	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	32.437	38.494	42.459	-	42.459	55.179	60.075	44.413	58.413	-	-
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	170.959	202.252	255.137	-	255.137	257.172	258.028	258.362	258.923	-	-
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	48.636	60.948	56.039	-	56.039	41.574	41.856	41.755	36.755	-	-
IT-05: *CYBER TECHNOLOGY*	-	63.891	39.664	0.000	-	0.000	0.000	0.000	0.000	0.000	-	-

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 and embedded computing systems.

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. The technologies will provide cost-effective security and survivability solutions that enable DoD information systems to operate correctly and continuously even under attack.

The Language Understanding and Symbiotic Automation project develops technologies to enable computing systems to understand human speech and extract information contained in diverse media; to learn, reason and apply knowledge gained through experience; and to respond intelligently to new and unforeseen events. Enabling computing systems in this manner is of critical importance because sensor, information, and communication systems generate data at rates beyond which humans can assimilate, understand, and act. Incorporating these technologies in military systems will enable warfighters to make better decisions in complex, time-critical, battlefield environments; intelligence analysts to make sense of massive, incomplete, and contradictory information; and unmanned systems to operate safely with high degrees of autonomy.

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Defense Advanced Research Projects Agency	Date: February 2016
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 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.

B. Program Change Summary ($ in Millions)	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Previous President's Budget	324.407	356.358	364.076	-	364.076
Current President's Budget	315.923	341.358	353.635	-	353.635
Total Adjustments	-8.484	-15.000	-10.441	-	-10.441
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	-15.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	1.831	0.000			
• SBIR/STTR Transfer	-10.315	0.000			
• TotalOtherAdjustments	-	-	-10.441	-	-10.441

Change Summary Explanation

FY 2015: Decrease reflects reprogrammings offset by the SBIR/STTR transfer.

FY 2016: Decrease reflects congressional reduction.

FY 2017: Decrease reflects completion of the Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) and Robust Automatic Translation of Speech (RATS) programs.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	32.437	38.494	42.459	-	42.459	55.179	60.075	44.413	58.413	-	-

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. The goal will be to create not just larger computing platforms, but to extract information out of large and chaotic data sets efficiently. One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build complex computing systems including software and hardware. 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 2015	FY 2016	FY 2017
Title: Complexity Management Hardware	7.500	11.194	10.000
Description: The battlefield of the future will have more data generators and sensors to provide information required for successful combat operations. With networked sensors, the variety and complexity of the information streams will be even further extended. The Complexity Management Hardware program will develop silicon designs which help alleviate the complexity inherent in next generation systems. These systems will have increasingly large data sets generated by their own multidomain sensors (such as RF and Electro-Optical/Infrared (EO/IR) payloads) as well as potentially new inputs from external sensors. With current programming approaches, there are laborious coding requirements needed to accommodate new data streams. Additionally, the context provided by these data sets is ever changing, and it is imperative for the integrated electronics to adapt to new information without a prolonged programming cycle. Providing contextual cues for processing data streams will alleviate the fusion challenges that are currently faced, and which stress networked battlefield systems. As opposed to the intuition and future-proofing that is required at the programming stage of a current system, the silicon circuit of the future will be able to use contextual cues to adapt accordingly to new information as it is provided. The applied research aspects of this program will investigate circuit design which can exploit the algorithms showing benefit for complexity management. This will entail various sparse versus dense data manipulations with hardware implementations catered			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
to both types of data. The program will show hardware implementations that gracefully handle multiple data streams and limit the programming burden for a complex scenario. Basic research efforts are funded in PE 0601101E, Project CCS-02. ***FY 2015 Accomplishments:*** - Designed complexity management processor algorithm and benchmark tests for object recognition in still images and action recognition in video. - Demonstrated critical features of algorithm including ability to learn and adapt while operating. - Quantified impact of using low precision, sparse network connectivity on accuracy of results. ***FY 2016 Plans:*** - Design transistor level circuits implementing the complexity management algorithms. - Demonstrate the ability to manage multiple data streams with interlaced information. - Create initial hardware verification of concepts for both sparse and hardware demonstrations. ***FY 2017 Plans:*** - Compare various algorithms ability to manage complex data sets. - Quantify the benefits of various architecture approaches to management of large data streams when overlaid with contextual information. - Translate the initial algorithms to high level circuit implementations to show the power and processing requirements.			
Title: Power Efficiency Revolution For Embedded Computing Technologies (PERFECT)	24.937	17.800	-
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 by developing approaches including 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 optimized data placement to provide the required embedded system processing power efficiency. The remaining efforts under the PERFECT program will emphasize the implementation of near threshold and specialization approaches to address processing efficiency. ***FY 2015 Accomplishments:***			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Incorporated test chip results - circuit, architecture, communication, power management, 3D - into design optimizations and simulation refinements for continuing architectural development efforts. - Developed compiler algorithms supporting communication-avoiding optimization, concepts for optimizing parallel codes, and programming language-based auto-tuning. - Delivered 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 released new hardware description language and modeling/simulation infrastructure incorporating the evaluation and development of algorithms, specializers, hardware architectures, and resiliency techniques. ***FY 2016 Plans:*** - Select implementation and transition targets. Establish a focused subset of PERFECT teams' technologies to most effectively support target requirements. - Integrate our modeling and evaluation environment by combining separate optimization tools for power, communication avoidance, and resiliency. This will provide detailed trade-off analyses for a range of (1) ISR kernels, (2) PERFECT hardware targets, and (3) problem instance sizes. This will support 20X power savings, while respecting resiliency requirements, relative to classical application implementations. - Demonstrate High Level Source-to-Source transformation targeting PERFECT program specialization simulators. Generate optimized/vectorized code exploiting explicit memory movement and dynamic voltage and frequency control for performance efficiency. These will be demonstrated on ISR kernels and convolutional neural networks. - Demonstrate near memory fast Fourier transform accelerator supporting synthetic aperture radar and space-time adaptive processing using PERFECT architecture simulator. - Fabricate 14nm (Global Foundry) test chips to measure ultra low voltage Static random-access memory implementations. Anticipated results include a functional voltage of 0.3 Volts, and a 3x access time improvement versus conventional approaches. - Demonstrate the benefits of specialization using the PERFECT Vision Chip by emulating the execution of major vision kernels with the expectation to attain peak efficiencies.			
Title: Portable AnaLyticS (PALS)* ***Description:*** *Formerly Scalable Optical Nodes for Networked Edge Traversal (SONNET) Graph analytics on large data sets is currently performed on leadership-class supercomputers that are designed for other purposes. These machines are required because they have the memory capacity required for large graph problems, but the ability to efficiently move data to and effectively utilize compute resources is limited, resulting in extremely low compute efficiency. Computationally, graph analysis is characterized by many short, random accesses to memory which is inefficient on current	-	3.500	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017

systems that are optimized for regular, predictable access. The movement of data between memory and processors now requires more time and energy than the logical operations themselves. This is the result of generations of systems that architecturally separate computing/data manipulation and main data storage. Large systems have shown utilization (percentage of system peak throughput capability used) drop from as high as 90% to in the order of 2% due to the data patterns for different applications. To resolve this problem, the PALS program will develop technologies, architectures, and software approaches that move critical data processing kernels and critical data organization operations adjacent to the memory itself, rather than at physically distant general computing nodes, addressing data latency, overall computational performance and power for critical data intensive elements of an application.

The PALS approach is not to physically or functionally move processing entirely to the memory, but rather to move specific, critical data intensive components of an application to the data. The result will dramatically improve performance for data intensive applications, by off-loading the main processor of data-intensive operations, and enabling data security operations at the memory itself. This will be accomplished by utilizing industry advances in 3D packaging, particularly the bandwidth, latency and power advances being developed in 3D memory stacks; new software approaches for data management; investigating alternative data movement technologies such as co-designing processor and photonic hardware, exploiting the high bandwidth provided by silicon photonics. It will also include incorporation of domain specific logic for unique and asymmetric data-intensive DoD functional capabilities at all appropriate levels of a processing system's memory. The performance and efficiency will be transformational for data analytics for both big data and embedded data-intensive DoD applications and enable real-time analysis on dynamic graphs in the fields of cyber security, threat detection, and numerous others.

FY 2016 Plans:

- Identify common graph primitives that would accelerate the execution of DoD-specific applications.
- Explore the applications benefitting from the unique architecture and whether unique hardware design allows for processors for unique military applications.
- Identify domain specific primitives that would accelerate performance by moving data-intensive functionality to appropriate processing system data storage levels and specifically a memory 3D stack logic layer.

FY 2017 Plans:

- Develop domain specific concepts for functionality at the hierarchical levels of data storage levels, define logic and data orchestration capabilities at these layers of storage and processing, define customization versus programmability trade-offs, and define logic layer processing concepts.
- Simulate performance of PALS for selected high value application specific and data-intensive applications.
- Develop initial architectural trade-offs and implementation options.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Develop PALS based security concepts for data management in multi-security level environments.			
Title: Electronic Globalization ***Description:*** Approximately 66% of all installed semiconductor wafer capacity is in Asia. This creates a significant risk for the DoD as off-shore manufacturing of microelectronic components could introduce various vulnerabilities to DoD systems that utilize these non-U.S. fabricated electronic components. As the DoD is faced with this globalization reality, it is essential to prevent potential consequences such as reverse engineering, and the theft of U.S. intellectual property. New applied research technology enablement will be developed in the Electronics Globalization program to provide a means of assessing the impact of high stress upon Government Off-The-Shelf (GOTS) and Commercial Off-The-Shelf (COTS) components produced in conventional contemporary foundries. The potential application of these components in extreme stresses DoD systems and makes it even more important to understand the new physics mechanisms to be expected in these regimes. The extendibility of existing reliability models, and the calibration of new reliability models for components operated outside of typical use conditions will be studied. Further, the insight gained from understanding these impacts will inform the use of elevated stress burn-in and screening tools, potentially allowing shorter and more effective test times in the fabrication plant. ***FY 2016 Plans:*** - Improve the signal-to-noise ratio of the Navy system, allowing its use in a wider array of microelectronic parts. - Study high stress effects on conventionally fabricated COTS and GOTS electronic components. - Develop device physics models which accurately capture the reliability physics behavior of semiconductors operated at elevated voltage and temperature. ***FY 2017 Plans:*** - Continue prototype system enhancements to the laser scanning tools. - Continue to study high stress effects on conventionally-fabricated COTS and GOTS electronic components. - Characterize the physics models using the response of the fabricated devices to extreme stress associated with certain DoD applications as well as accelerated life stress testing and evaluation. - Complete the development of shorter, more effective reliability screens and burn-in testing using higher stress test conditions.	-	4.000	4.000
Title: tactical CONtext EXtraction (CONEX) ***Description:*** Enriching a primary data stream with contextual information (i.e., the circumstances or facts such as who, what, and where that surround a particular event) can be accomplished by fusing data from multiple sensors. For this task, modern systems rely heavily on man-made reference signals, such as Global Positioning Systems (GPS), and preprogrammed algorithms with limited adaptability. Object recognition using Deep Learning and related approaches has been demonstrated, but these methods	-	-	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
require significant offline training. The tactical CONtext EXtraction (CONEX) program will develop compact sensors and adaptive processors for extracting contextual information from resource-constrained environments. CONEX sensors will collect information from the landscape and natural sources, such as the relative position of stars, to supplement inertial measurement systems and other sensor feeds in GPS-denied areas. CONEX processors will contain embedded real-time learning algorithms that operate over multiple timescales. These adaptive methods efficiently capture complex spatial and temporal structure in noisy, ambiguous data streams that are beyond the analysis capabilities of state-of-the-art signal/image processing systems. ***FY 2017 Plans:*** - Refine designs of integrated circuits that implement real-time learning algorithms. - Design compact, low-power CONEX sensors to support context accumulation in selected environments. - Demonstrate performance enhancement of novel content extraction algorithms and software. - Demonstrate basic functionality of prototype CONEX sensors.			
Title: Removing Barriers to Hardware (REBHAR) ***Description:*** Small software companies are a dynamic force in the U.S. economy because they face very low barriers to innovation. Anyone can code applications for established mobile or cloud platforms and leverage the tremendous infrastructure built by larger companies to quickly access potential customers. However, commercial hardware innovations for advanced integrated circuits and Micro-Electro-Mechanical Systems (MEMS) sensors face costly obstacles that impede progress outside of large corporations. Smaller businesses generally do not have the budget or sales volume to access the latest design software, verification tools and fabrication processes. The smaller DoD market for hardware amplifies these problems for delivering revolutionary military components. The Removing Barriers to Hardware (REBHAR) program will develop methods to facilitate hardware innovation for defense applications. The objective of the REBHAR program is to establish relationships with commercial companies to gain access to proven processes, to explore the possibilities of open source hardware, and to develop an aftermarket customization strategy to economically adapt commercial chips to specific military needs. ***FY 2017 Plans:*** - Explore the concept of open source design kits and open source hardware development cycles. - Demonstrate methods for aftermarket customization of commercial integrated circuits for select defense applications. - Demonstrate circuits based on open source design kits.	-	-	6.000
Title: Spectrum Grand Challenge ***Description:*** The objective of the Spectrum Grand Challenge is for participants to develop wireless communications networks which can learn to cohabitate and share the same Radio Frequency (RF) spectrum as other networks without preplanning or co-	-	2.000	10.459

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
design of the technologies. Access to spectrum is critical to many modern sectors: military, commercial, infrastructure, public-safety, disaster recovery, and many more. Spectrum however is treated as a scarce resource typically assigned to exclusive-use licenses. These approaches still rely on exclusive use of the spectrum by only a single network. In order to meet growing spectrum demands networks must be able to dynamically adapt their use of the spectrum as needs and as spectrum conditions change, autonomously determining when, where, and how spectrum should be used. Spectrum Grand Challenge solutions will survey their environment, learn to morph their configuration to suit both their needs and others, and employ interference coping and exploitation techniques to make more efficient use of the RF spectrum. The Spectrum Grand Challenge will develop the world's first large-scale spectrum testbed to test participants in realistic emulated conditions. The test conditions and qualification metrics developed will thoroughly vet solutions, and ultimately serve as the basis for certification of an envisioned new class of shared spectrum technology which does not rely on exclusive use of the spectrum. This program complements spectrum access and wireless communications work in PE 0603760E, Project CCC-02. ***FY 2016 Plans:*** - Define Spectrum Grand Challenge rules governing eligibility as well how the competition will be conducted and scored. ***FY 2017 Plans:*** - Design and build out large-scale spectrum testbed for use in the preliminary competition of the Spectrum Grand Challenge. - Hold qualifying event to select field of participants. - Hold preliminary competition in an emulated RF environment using spectrum sharing testbed.			
Accomplishments/Planned Programs Subtotals	32.437	38.494	42.459

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 2017 Defense Advanced Research Projects Agency			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	170.959	202.252	255.137	-	255.137	257.172	258.028	258.362	258.923	-	-

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. The technologies will provide cost-effective security and survivability solutions that enable information systems to operate correctly and continuously while under attack and to be rapidly recovered/reconstituted in the aftermath of an attack. Technologies developed by 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 2015	FY 2016	FY 2017
Title: Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)	11.500	22.000	29.938

Description: The Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) program is developing technologies to enable reliable communications for military forces that operate in the presence of disrupted, degraded or denied wide-area networks. The program is creating algorithms and software prototypes for use exclusively at the network edge, specifically, on end hosts and/or on proxy servers (middleboxes) fronting groups of such end hosts within a user enclave. EdgeCT systems will sense and respond rapidly to network failures and attacks by dynamically adapting protocols utilized to exchange packets among these hosts, thereby implementing fight-through strategies that restore networked communication. This will enable highly reliable networked communication for the military in the face of a wide variety of common network failure modes as well as cyber attacks against network infrastructure. EdgeCT technologies will be developed in collaboration with and transitioned to operational commands.

FY 2015 Accomplishments:

- Formulated a distributed architecture for reliable communications over high-speed wide-area networks that have been degraded by cyber attack, misconfiguration, or hardware/software failure.
- Introduced techniques to sense and respond rapidly to network failures and attacks by dynamically adapting protocols utilized to exchange packets among hosts.
- Created an initial wide-area network testbed enabling joint experimentation and demonstration of components and systems among program performers.

FY 2016 Plans:

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Develop fight-through strategies that rapidly restore networked communication in the face of a wide variety of common network failure modes as well as cyber attacks against network infrastructure. - Demonstrate performance at the component and subsystem levels, to include real-time network analytics, holistic decision systems, and dynamically configurable protocol stacks. - Assess EdgeCT component and system designs for potential weaknesses, vulnerabilities, and countermeasures associated with cyber attacks against network infrastructure, or against EdgeCT systems themselves. - Initiate development of software prototypes suitable for laboratory experimentation with operational commands. - Explore modes of user interaction and system concepts of operation with one or more operational commands and bring software prototypes to an initial field experiment in collaboration with an operational command. ***FY 2017 Plans:*** - Demonstrate and evaluate system prototypes against program metrics to verify adequate performance for cumulative network utility, recovery time, and network overhead. - Increase the number of enclaves and total application data flows that can be accommodated during real-time operation. - Incorporate military applications, such as Command and Control (C2) software systems, into system demonstrations. - Extend usage and testing scenarios to include multiple forms of simultaneous failures and cyber attacks within the wide area network.			
Title: Cyber Fault-tolerant Attack Recovery (CFAR) ***Description:*** The Cyber Fault-tolerant Attack Recovery (CFAR) program is developing novel architectures to achieve cyber fault-tolerance with commodity computing technologies. Current approaches to handling cyber-induced faults in mission-critical systems are inadequate, as perimeter defenses wrapped around vulnerable monocultures do not scale, while zero-day exploits evade signature-based defenses. The proliferation of processing cores in multi-core central processing units provides the opportunity to adapt fault-tolerant architectures proven in aerospace applications to mission-critical, embedded, and real-time computing systems. The CFAR program will combine techniques for detecting differences across functionally replicated systems with novel variants that guarantee differences in behavior under attack. The resulting CFAR-enabled computing systems will quickly detect deviations in processing elements at attack onset and rapidly reboot to restore affected services. ***FY 2015 Accomplishments:*** - Formulated a novel architecture that can achieve cyber fault-tolerance with commodity computing technologies without requiring changes to the system concept of operations. - Developed initial techniques for detecting differences across functionally replicated systems. - Developed initial techniques for producing novel compiled software variants that behave differently under attack. ***FY 2016 Plans:***	10.500	20.149	27.494

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Demonstrate functionally replicated systems and novel variants that provide performance close to optimal and exhibit sufficient variability to guarantee differences in behavior under attack. - Implement and test techniques for quickly detecting differences across replicated systems. - Implement and evaluate alternative architectures for achieving cyber fault-tolerance for mission-critical military applications with commodity computing technologies. - Work with potential transition sponsors to evaluate military computing systems as candidates for technology refresh with CFAR technologies. ***FY 2017 Plans:*** - Create variants from binary code, which will enable the technology to protect systems for which source code is not readily available. - Develop methods to produce mathematical proofs of semantic equivalence across variants, which will contribute to assurance cases that systems protected with CFAR technology behave identically to the original unprotected systems. - Develop robust cyber fault-tolerant models that, unlike conventional approaches to physical fault tolerance, handle the highly correlated and frequent faults that may result from a cyber-attack. - Demonstrate proof-of-concept on a representative mission system, showing that the system behaves identically to the original while providing protection and rapid recovery from cyber attacks.			
Title: Supply Chain Hardware Integrity for Electronics Defense (SHIELD)	17.750	21.000	24.500
Description: Counterfeit electronic components compromise business as well as defense systems, 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 exhibited limited effectiveness. 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 of these methods are specific to a manufacturer's component and as such address only those issues critical to that manufacturer. Some methods can be circumvented, or require slow, expensive, off-site forensic analysis to verify authenticity. The Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program will develop a technology capable of confirming, at any time and place, the authenticity of 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 encrypted ID as well as anti-tamper features. The			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
microscopic-size dielet embedded in the electronic component packaging will enable verification of a chip's identity from very close proximity. ***FY 2015 Accomplishments:*** - Refined design specifications and technical requirements for the SHIELD dielet, including Advanced Encryption Standard counter with Cipher Block Chaining Message Authentication Code (AES CCM) as the target encryption protocol. - Developed behavioral models for dielet power and communications to support preliminary design efforts. - Manufactured "surrogate" dielets with the dimensions and form factor of the SHIELD design for performers to develop package insertion methods and fragility testing. - Designed and manufactured hardware test sites to demonstrate proof of concept for key dielet technologies (sensors, power, communications, encryption, dielet fragility). ***FY 2016 Plans:*** - Refine designs based on measured results from test site hardware. Scale proof-of-concept work done at less advanced design nodes to the 40 nanometer and 14 nanometer target design nodes for SHIELD. - Design and manufacture hardware test sites to demonstrate second pass improvements for key dielet technologies. - Develop transaction model for reader-to-dielet interrogation. - Select best-fit Phase 1 technologies for inclusion on Phase 2 dielet designs, based on validated hardware measurements and objective analysis of design compatibility. - Refine dielet singulation, test and insertion methodology and fragility design based on mechanical testing of surrogate dielets. ***FY 2017 Plans:*** - Design and manufacture prototype SHIELD dielets, integrating best-fit technologies selected during Phase 1. - Implement dielet singulation method for wafers after manufacture. - Initiate functional and performance testing of manufactured SHIELD dielets. - Refine methods for dielet insertion into integrated circuit (IC) packages. - Build and test network appliance and server network for Phase 3 testing.			
Title: Brandeis* ***Description:*** *Previously Adaptable Information Access and Control (AIAC) The Brandeis program is creating the capability to dynamically, flexibly, and securely share information while ensuring that private data may be used only for its intended purpose and no other. In the civilian sphere, there is a recognized need for technologies that enable the sharing of information between commercial entities and U.S. government agencies. Similarly, the U.S. military is increasingly involved in operations that require highly selective sharing of data with a heterogeneous mix of allies, coalition	7.593	17.600	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
partners, and other stakeholders. The Brandeis program will develop the technical means to protect the private and proprietary information of individuals and enterprises. Brandeis will break the tension between (a) maintaining privacy and (b) being able to tap into the huge value of data. Rather than having to balance between them, Brandeis aims to build a third option: enabling safe and predictable sharing of data in which privacy is preserved. The Brandeis program is timely due to recent progress on techniques such as homomorphic encryption, secure multiparty computation, and differential privacy. To facilitate deployment, Brandeis 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 Accomplishments:*** - Formulated technical approaches to data privacy through secure multiparty computation, secure database queries, differential privacy and remote attestation of protected computing environments. - Identified canonical privacy use cases on which to evaluate candidate privacy technologies. - Conceptualized prototype evaluation platforms and metrics/analysis tools on which privacy technologies can be tested and metrics computed to quantify the privacy benefits. ***FY 2016 Plans:*** - Implement secure multiparty computation, secure database queries, differential privacy and remote attestation techniques in initial prototypes suitable for integration on commodity cloud infrastructures. - Develop prototype evaluation platform and metrics/analysis tools on which privacy technologies can be tested and metrics computed. - Initiate quantification of privacy benefits of privacy technologies in the context of canonical individual and enterprise privacy use cases. ***FY 2017 Plans:*** - Optimize privacy prototypes that implement secure multiparty computation, secure database queries, differential privacy and remote attestation techniques and test on enterprise networks. - Quantify privacy benefits and the costs in terms of computational overhead and latency. - Perform detailed studies of the security implications of the techniques in terms of confidentiality, integrity, and availability of private information. - Initiate transition of techniques through integration on commercial, coalition partner, and military enterprise networks.			
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)* ***Description:*** *Previously Protecting Cyber Physical Infrastructure	7.525	17.513	24.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program will create new technologies for maintaining the availability and integrity of critical U.S. cyber-physical infrastructure. This is a national security issue due to the near-ubiquitous use of computers to monitor and control U.S. civilian and military critical infrastructure such as electric power. RADICS will develop technologies to monitor heterogeneous distributed control system networks, detect anomalies that require rapid assessment, isolate compromised system elements, characterize attacks in real time, mitigate sensor spoofing and denial of service attacks, and restore services. Hardware-in-the-loop simulation techniques will be developed to enable the discovery of emergent vulnerabilities and the development and optimization of mitigation, restoration, and reconstitution strategies applicable to the power grid. This will include understanding the potential role of electric power markets and smart grid technologies in propagating or damping power grid anomalies. RADICS technologies will transition to military installations and commercial industry. ***FY 2015 Accomplishments:*** - Formulated resilient architectures for real-time monitoring, analysis, and assessment of distributed industrial control systems and physical infrastructure. - Investigated rapid re-provisioning techniques to quickly re-deploy firmware and operating system images to restore compromised devices back to a pristine, known state of operation. ***FY 2016 Plans:*** - Create a hardware-in-the-loop simulation capability to enable the discovery of emergent vulnerabilities and the development and optimization of mitigation strategies applicable to the U.S. power grid. - Develop technologies to monitor heterogeneous distributed industrial control system networks, detect anomalies that require rapid assessment, mitigate sensor spoofing and denial of service attacks, and restore services. - Extend simulation capabilities to understand the potential role of electric power markets in propagating or damping power grid anomalies. - Develop techniques that use organic sensors, remote instrumentation, and other sources of cyber situation awareness information to continuously optimize cyber defenses. ***FY 2017 Plans:*** - Validate emulations of embedded industrial control devices for development, test and evaluation of defensive cyber measures. - Explore techniques to enable validated dynamic simulations of cascading faults across large sections of a power grid. - Develop the means to produce a robust, multi-source time base with sufficient accuracy to enable continued operation of critical infrastructure in the event of a disruption of GPS signals. - Develop defense mechanisms for supervisory control and data acquisition systems that are subject to systematic/malicious attack in addition to random perturbations/failures.			
Title: High Assurance Cyber Military Systems	24.000	27.690	17.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
Description: The High Assurance Cyber Military Systems (HACMS) program is developing and demonstrating technologies 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, 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 2015 Accomplishments:*** - Formally verified full functional correctness for the extended core operating system and the automatically synthesized control systems for selected vehicles. - Demonstrated required security properties that follow from correctness for the extended core operating system and the automatically synthesized control systems. - Performed static and dynamic assessments after modifications were made on militarily-relevant vehicles to evaluate the effectiveness of the synthesis and formal methods tools. - Conducted a field test of a HACMS hardened operating system integrated in a helicopter mission computer during which live cyber attacks on unsecured applications were contained. ***FY 2016 Plans:*** - Apply an architecture-based approach to high-assurance system development to develop a large fraction of the software for a two-processor open-source quadcopter, a helicopter, an unmanned wheeled robot, and a military transport vehicle. - Demonstrate machine-tracked assurance cases for system-wide security properties on targeted vehicles. - Increase the level of automation of proof generation in theorem provers. - Evaluate the effectiveness of approaches by conducting penetration-testing exercises on the targeted vehicles. ***FY 2017 Plans:*** - Develop techniques for ensuring the predictable composability of adaptively assembled systems. - Formulate assurance cases for complex mission critical systems that are comprised of multiple interacting components. - Develop formal methods approaches to enable predictable system design at scale. - Evaluate the effectiveness of the formal methods approaches by conducting penetration-testing exercises.			
Title: Vetting Commodity Computing Systems for the DoD (VET)	21.987	22.625	18.019

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
Description: The Vetting Commodity Computing Systems for the DoD (VET) program is developing 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 detect hidden malicious functionality and also enable the detection of software and firmware defects and vulnerabilities that can facilitate adversary attack. ***FY 2015 Accomplishments:*** - Improved the effectiveness of prototype tools, in particular by reducing the rates of false alarms and missed detections, through further competitive engagements. - Expanded the set of challenge programs to explore more complex forms of malicious hidden functionality including race conditions, information leakage, and defective encryption. - Replaced initial experimental platforms with more complex devices that are more operationally representative. ***FY 2016 Plans:*** - Measure probabilities of false- and missed-detection and human analysis time to identify new techniques that are likely candidates for integration into an end-to-end DoD vetting application. - Initiate development of an integrated vetting application that incorporates the most promising new techniques and scales to problems of operationally relevant size. - Conduct an integrated end-to-end software/firmware-vetting technology demonstration relevant to potential transition partners. ***FY 2017 Plans:*** - Run comparative performance evaluations between program-developed vetting tools and commercially available tools. - Engage in experiments and pilot deployments of prototype tools with transition partners on software of interest to DoD. - Based on user feedback, make improvements to prototypes to enhance usability in the context of vetting software for DoD.			
Title: Cyber Grand Challenge (CGC)	6.233	11.329	11.000
Description: 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. Initial funding for this effort was			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
provided in Project IT-05. Additional funding is being provided in IT-03 to enable the creation of the more robust competition infrastructure necessary to accommodate the large number of competitors. ***FY 2015 Accomplishments:*** - Created the robust competition infrastructure required to accommodate the large number of competitors. ***FY 2016 Plans:*** - Conduct world's first automated computer security contest: Cyber Grand Challenge Final Event. - Release event results as cyber research corpus to measure and challenge future automated cyber capabilities. ***FY 2017 Plans:*** - Use the lessons learned from the (first) Cyber Grand Challenge Final Event to design a follow-on competition in which competitor systems compete directly against experts. - Benchmark and baseline the abilities of expert reverse engineers to guide the creation of a machine-vs-expert competition corpus. - Initiate development of a competition infrastructure that allows for distributed machine-vs-expert tournament play.			
Title: Extreme Distributed Denial of Service Defense (XD3) ***Description:*** Building upon work in the Mission-oriented Resilient Clouds (MRC) program, the Extreme Distributed Denial of Service Defense (XD3) program will develop new computer networking architectures better able to deter, detect, and overcome distributed denial of service (DDoS) attacks. DDoS attacks include not only high-volume flooding attacks of hundreds of gigabits per second, but more subtle low-volume attacks that evade traditional intrusion detection systems while causing exhaustion of server processor and memory capacity. These attacks will likely accelerate as the Internet of Things (IoT) expands to new classes of devices that in many cases will be deployed with inadequate security controls: attackers will incorporate poorly defended IoT devices in their botnets. XD3 will develop defensive architectures that use maneuver, deception, dispersion, and on-host adaptation to increase adversary work factors, boost resilience of mission critical services such as command and control, and ultimately thwart DDoS attacks. ***FY 2016 Plans:*** - Formulate architectures and algorithms that enable physical and/or logical dispersion of likely DDoS targets (e.g., servers and cloud computing facilities) to complicate the location and targeting of these cyber resources by DDoS attackers. - Develop network maneuver and deception techniques that increase adversary work factors in target development, attack planning, and execution.	-	14.996	26.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Devise means for enabling servers and similar DDoS targets to sense the presence of DDoS attacks (especially low-volume attacks) and to adapt their operation in real time to mitigate the attack while preserving performance for legitimate users. ***FY 2017 Plans:*** - Develop testing capabilities to support iterative experimentation and demonstration of prototypes. - Implement and integrate network dispersion, maneuver, and deception techniques in prototype systems that increase adversary work factors in target development, attack planning, and execution. - Perform system-level demonstrations and subject systems to critical assessments to pinpoint design weaknesses and vulnerabilities. - Conduct military field exercises in collaboration with transition partners to elicit feedback on XD3 features, capabilities, and concepts of operation.			
Title: Leveraging the Analog Domain for Security (LADS) ***Description:*** The Leveraging the Analog Domain for Security (LADS) program, building upon the Vetting Commodity Computing Systems for the DoD (VET) program, will develop and demonstrate techniques for defending information systems using side channel signals such as radio frequency and acoustic emissions, power consumption, heat generation, differential fault analysis, and timing-based effects. LADS augments standard cybersecurity approaches, which focus on digital effects/phenomena, with analog techniques. LADS will enable defenders to detect cyber attacks by sensing changes in the analog emissions of computing components, devices, and systems, greatly complicating the task of adversaries who wish to remain covert. ***FY 2016 Plans:*** - Formulate approaches for measuring side channel signals such as radio frequency and acoustic emissions, power consumption, heat generation, differential fault analysis, and timing-based effects in noisy environments. - Investigate rule-based and statistical classification techniques for discriminating side channel signals emitted from computing components, devices, and systems operating in compromised/faulty states from those operating in secure/correct states. - Propose approaches for predicting side channel emissions given knowledge of the computing system hardware and executed code. ***FY 2017 Plans:*** - Develop quantitative models for side channel signals emitted from systems operating in secure/correct states and from systems operating in compromised/faulty states and validate the models through laboratory measurements. - Assess the practicality of initial techniques for discriminating side channel signals emitted from systems operating in compromised/faulty states from those operating in secure/correct states by computing receiver operating characteristics (probability of detection versus probability of false alarm).	-	10.000	19.000

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Develop statistical models for side channel emissions given imprecise/probabilistic knowledge of the executed code.			
Title: Plan X ***Description:*** The Plan X program is developing 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 is creating 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. Initial funding for this effort was provided in Project IT-05. Funding continues in IT-03 for testing and evaluation through participation in tactical level exercises and integrating the Plan X system into transition partner operating profiles. ***FY 2017 Plans:*** - Refine Plan X capabilities to provide operators with enhanced cyber situational awareness and to enable operators to execute cyber warfare missions with projections of cyber collateral damage. - Demonstrate capabilities in multiple military cyber exercises, such as Cyber Guard, Cyber Flag, and Red Flag. - Refine operator workflows and operational use cases based on exercise feedback. - Work with transition partners, such as U.S. Cyber Command (USCYBERCOM) and U.S. Army Cyber Command (ARCYBER), to integrate Plan X into current operating systems.	-	-	23.349
Title: System Security Integrated Through Hardware and software (SSITH) ***Description:*** System Security Integrated Through Hardware and software (SSITH) seeks to better protect DoD systems by exploring innovative approaches that combine hardware and software to provide enhanced system security. Traditional cybersecurity approaches have focused either on software or hardware, but rarely on an integration of both domains. By exploring integrated hardware/software solutions, SSITH will combine the efficiency and robustness of hardware with the flexibility and adaptability of software to provide security solutions that are resistant to attack and adaptive to new attack approaches. The program is based on the concept that co-design of hardware and software provides new modalities to protect electronic systems. The SSITH program will pursue several hardware/software approaches to enhancing electronic system security. First, the program will investigate new co-designed hardware/software architectures that are inherently more secure than current electronic systems. Second, the program will investigate hardware/software architectures that are flexible and can adapt to new system attack methods and vectors. Third, the program will examine methods to reduce the power/performance overhead required to implement novel and powerful protection methods recently conceived in the security community.	-	-	8.337

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
FY 2017 Plans: - Define new hardware/software architectures that implement flexible and robust protection against external attack. - Utilize modeling and simulation approaches to determine the expected improvement in protection of the new hardware/software architectures relative to software only and hardware only approaches.			
Title: Mission-oriented Resilient Clouds (MRC)	15.892	8.750	-
Description: The Mission-oriented Resilient Clouds (MRC) program is creating 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 is addressing this risk by creating advanced network protocols and new approaches to computing in potentially compromised distributed environments. Particular attention is focused on adapting defenses and allocating resources dynamically in response to attacks and compromises. MRC will result in new approaches to measure trust, reach consensus in compromised environments, and allocate 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 2015 Accomplishments:*** - Demonstrated automated construction of diverse, redundant network flow paths that maximize communication resilience in clouds. - Evaluated and measured the scalability and resilience of a high-assurance cloud computing application development library in terms of number of concurrent replicas supported and volume of data handled. - Developed and demonstrated hardened network services through fine-grained memory access controls that determine what valid memory addresses are read or written to by each instruction in a program. - Demonstrated concurrent optimization of computing resources and network bandwidth to achieve significant reduction in network load with no performance loss. - Inserted and evaluated multiple MRC technologies into U.S. Pacific Command (USPACOM) distributed computing environments. - Assessed technologies with Defense Information Systems Agency (DISA) to facilitate transitions into DoD networks and clouds. ***FY 2016 Plans:*** - Demonstrate correct, disruption-free upgrading of software defined networking controllers in live networks. - Complete transition of one or more technologies into operational use by USPACOM and DISA. - Transition secured version of multi-UAV control software to Air Force Research Laboratory (AFRL).			
Title: Active Cyber Defense (ACD)	13.828	8.600	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
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 increase their work factor by limiting success from their efforts. ***FY 2015 Accomplishments:*** - Completed development of system components. - Performed a limited capability demonstration at CYBERFLAG 15-1 training exercise by successfully defending a targeted network enclave from attack. - Began integration of technologies into complete prototype platforms. - Tested integrated capabilities in collaboration with Director, Operational Test and Evaluation (DOT&E). ***FY 2016 Plans:*** - Complete integration of system platforms 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 to facilitate transition to DoD cyber operators.			
Title: Rapid Software Development using Binary Components (RAPID) ***Description:*** The Rapid Software Development using Binary Components (RAPID) program developed 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, potentially impacting operations. Advanced technology development for the program was budgeted in PE 0603760E, Project CCC-04. ***FY 2015 Accomplishments:*** - Developed new software component reuse capabilities to extend application performance to a wider range of realistic scenarios and enable an expanded concept of operations. - Implemented new capabilities in modules designed to interoperate seamlessly with deployed RAPID prototype systems. - Integrated new modules into prototype RAPID systems deployed at transition partner sites and supported initial operations.	10.396	-	-
Title: Active Authentication	7.025	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
Description: The Active Authentication program developed more effective user identification and authentication technologies. Current authentication approaches are typically based on long, complex passwords and incorporate no mechanism to verify that the user originally authenticated is the user still in control of the session. The Active Authentication program addressed these issues by focusing on the unique aspects of the individual (i.e., the cognitive fingerprint) through the use of software-based biometrics that continuously validate the identity of the user. Active Authentication integrated multiple biometric modalities to create an authentication system that is accurate, robust, and transparent to the user. ***FY 2015 Accomplishments:*** - Demonstrated multiple authentication biometrics suitable for deployment on desktop and mobile hardware for potential use by the DoD. - Prototyped an authentication platform suitable for use on desktop and mobile hardware in collaboration with potential transition sponsors. - Proved flexibility of the underlying prototype platform by creating an additional authentication platform suitable for DoD.			
Title: Anomaly Detection at Multiple Scales (ADAMS) ***Description:*** The Anomaly Detection at Multiple Scales (ADAMS) program developed and applied algorithms for detecting anomalous, threat-related behavior of systems, individuals, and groups over hours, days, months, and years. ADAMS developed flexible, scalable, and highly interactive approaches to extracting actionable information from information system log files, sensors, and other instrumentation. ADAMS integrated these anomaly detection algorithms to produce adaptable systems for timely insider threat detection. ***FY 2015 Accomplishments:*** - Developed techniques for representing end-user knowledge and feedback to ensure that the machine learning algorithms are working with the most effective features possible. - Demonstrated and quantified performance of algorithms in a series of controlled tests on blended synthetic/real data. - Hardened prototypes and installed these in operational environments for testing and evaluation.	7.000	-	-
Title: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) ***Description:*** The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program developed 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 developed mechanisms at the hardware and operating system level that eliminate known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH also developed software techniques that allow a computer system	6.730	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH developed techniques that make each computer system appear unique to the attacker and allow each system to change over time. ***FY 2015 Accomplishments:*** - Produced a hardened web server and browser that enable the creation of secure web applications from untrusted code. - Initiated two international standards submissions for securing web browsers and their communications. - Demonstrated policy-based application monitoring and hardware-assisted self-healing of multiple applications and hardware-based detection of malicious software. - Developed and demonstrated automated code randomization techniques to implement moving target defenses for software. - Developed and commercialized technology to detect hardware trojans in field programmable gate array (FPGA) components and provide host protection for embedded devices, including routers, printers and Voice over Internet Protocol (VoIP) phones.			
Title: Integrated Cyber Analysis System (ICAS) ***Description:*** The Integrated Cyber Analysis System (ICAS) program developed 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 technologies facilitate 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 2015 Accomplishments:*** - Developed and implemented algorithms for automatically identifying and quantifying specific security risks on enterprise networks. - Conducted initial technology demonstrations including automatic indexing of data sources, common language integration, and reasoning across federated databases. - Integrated, evaluated, and optimized algorithms via testing against attacks/persistent threats provided by transition partners. - Completed fully functional beta versions of the applications with operational stability suitable for testing at transition partner locations.	3.000	-	-
Accomplishments/Planned Programs Subtotals	170.959	202.252	255.137

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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*

C. Other Program Funding Summary ($ in Millions)

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 2017 Defense Advanced Research Projects Agency			Date: February 2016
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-04 / *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	

COST ($ in Millions)	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	48.636	60.948	56.039	-	56.039	41.574	41.856	41.755	36.755	-	-

A. Mission Description and Budget Item Justification

The Language Understanding and Symbiotic Automation project develops technologies to enable computing systems to understand human speech and extract information contained in diverse media; to learn, reason and apply knowledge gained through experience; and to respond intelligently to new and unforeseen events. Enabling computing systems in this manner is of critical importance because sensor, information, and communication systems generate data at rates beyond which humans can assimilate, understand, and act. Incorporating these technologies in military systems will enable warfighters to make better decisions in complex, time-critical, battlefield environments; and allow intelligence analysts to make sense of massive, incomplete, and contradictory information; and unmanned systems to operate safely with high degrees of autonomy.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
Title: Low Resource Languages for Emergent Incidents (LORELEI)	17.875	22.225	28.620

Description: The Low Resource Languages for Emergent Incidents (LORELEI) program is developing the technology to rapidly field machine translation capabilities for low-resource foreign languages. The United States military operates globally and frequently encounters low-resource languages, i.e., languages for which few linguists are available and no automated human language technology capability exists. Historically, exploiting foreign language materials required protracted effort, and current systems rely on huge, manually-translated, manually-transcribed, or manually-annotated data sets. As a result, systems currently exist only for languages in widespread use and in high demand. LORELEI will take a different approach by leveraging language-universal resources, projecting from related-language resources, and fully exploiting a broad range of language-specific resources. These capabilities will be exercised to rapidly provide situational awareness based on information from any language in support of emergent missions such as humanitarian assistance/disaster relief, terrorist attack response, peacekeeping, and infectious disease response.

FY 2015 Accomplishments:
- Explored techniques for optimizing combinations of existing resources to eliminate reliance on large parallel corpora.
- Proved viability of techniques to identify and link mentions of entities from text in a low-resource language to a knowledge base.
- Developed methodologies for generating morphological variants of a word and for clustering entity mentions.

FY 2016 Plans:
- Develop initial techniques for quantifying the linguistic similarity of language usage in diverse documents and media.
- Develop algorithms to exploit the universal properties of languages when rapidly ramping up for a low-resource language.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
- Develop semantic techniques for identifying the common topics, themes, and sentiment in speech and text in diverse foreign languages. - Collect, generate, and annotate data for an initial set of resources in typologically representative medium-resource languages. - Create a baseline toolkit to rapidly develop an initial situational awareness capability given a new low-resource language document collection. ***FY 2017 Plans:*** - Develop means to determine opinions and beliefs in low-resource languages. - Construct an integrated system employing multiple algorithms for low-resource language analysis. - Develop the user interface platform that will provide native speaker information to the analysis platform and provide query-driven information to the users. - Evaluate the performance of the analysis algorithms on two new languages and measure progress on the languages evaluated in the previous year. - Work with end users to utilize and evaluate the interface platform.			
Title: Deep Exploration and Filtering of Text (DEFT) ***Description:*** The Deep Exploration and Filtering of Text (DEFT) program is developing language technology to enable automated extraction, processing, and inference of information from text in operationally relevant application domains. A key DEFT emphasis is to determine explicit and implicit meaning in text through probabilistic inference, anomaly detection, and other techniques. 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 reports, messages, or other documents. DEFT will extract knowledge at scale for open source intelligence and threat analysis. Planned transition partners include the intelligence community and operational commands. ***FY 2015 Accomplishments:*** - Developed technology for extracting belief, sentiment and intent, for representing geo-spatial features and temporal events, and for inference from a set of documents. - Integrated multiple complementary algorithms into a comprehensive and consistent functional suite to support end-user workflows and problems. - Focused algorithm development on knowledge base representation in preparation for embedding algorithms in workflows to enable reasoning and downstream analysis. - Initiated work to adapt algorithms to specific foreign languages. - Conducted performance evaluations on event representation and other aspects of knowledge base population.	23.933	30.223	17.419

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
- Transitioned multiple algorithms and conducted effectiveness assessments at multiple end-user sites. ***FY 2016 Plans:*** - Improve algorithm performance on current functions and expand to new functions such as extending currently single-document algorithms to function across multiple documents. - Improve the discovery of different ways in which names of people and other entities are expressed across multiple documents, and develop techniques for linking them together. - Merge and optimize combined output of algorithms focused on different tasks such as belief and sentiment extraction, event argument and attribute identification, and relation mapping. - Develop methods for evaluating the effectiveness of various natural language processing algorithms in a multi-lingual environment, including evaluation of sentiment and belief analysis. - Transition an initial system-level prototype and additional component prototypes to end-user sites for effectiveness assessment. - Refine areas of focus based on results of transition site evaluations and open evaluation performance. ***FY 2017 Plans:*** - Develop algorithms to detect sub-events and identify their relationships to main events. - Evaluate the accuracy and effectiveness of language processing in specific foreign languages. - Develop algorithms to combine information from multiple language sources. - Transition a multi-lingual system-level prototype to end-user sites for effectiveness assessment.			
Title: Robust Automatic Transcription of Speech (RATS) ***Description:*** The Robust Automatic Transcription of Speech (RATS) program is developing robust speech processing techniques for 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. Techniques of interest include speech activity detection, language identification, speaker identification, and keyword spotting. RATS technology is being developed and optimized on real world data in conjunction with several operational users. ***FY 2015 Accomplishments:*** - Developed new methods for field adaptations, which include lightly supervised and unsupervised adaptation of the algorithms to new channels and environments. - Developed methods for coping with extraneous signals found in field data. - Developed techniques to reduce the data required to adapt algorithms to new channels from hours to minutes.	6.828	8.500	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
- Produced a software integrated platform with a set of Application Programming Interfaces (APIs) and Graphical User Interfaces (GUIs) to be inserted at DoD and intelligence community partner sites and tested in the working environment of the partners. ***FY 2016 Plans:*** - Develop, integrate and test techniques to deal with multiple speakers and overlapping speaker channels. - Collect and annotate additional field collected data. - Develop unified API and interface to support multiple tactical integration platforms. - Integrate technologies in transition partner platforms, adjusting systems to fit partner needs. - Evaluate technologies on specialized operational scenarios.			
Title: Understanding Machine Intelligence (UMI) ***Description:*** The Understanding Machine Intelligence (UMI) program will develop techniques that enable artificial intelligence (AI) systems to better support users through transparent operation. If current trends continue, future U.S. military autonomous systems will need to perform increasingly complex and sensitive missions. AI will be critical to such autonomous systems, but in order for developers, users, and senior leaders to feel confident enough to deploy and use AI-enabled systems, they must operate with high degrees of transparency, reliability, predictability, and safety. UMI will develop AI technologies that support transparency by providing supporting rationale and logic sequences that establish the basis for and reliability of outputs. In addition, efforts will be made to develop a mathematically rigorous virtual stability theory for AI-enabled systems analogous to the (conventional) stability theory developed for dynamical systems (solutions to systems of differential equations). Such a virtual stability theory will enable the creation of feedback mechanisms that flag, interrupt, and modify anomalous outputs and behaviors to ensure safe, predictable operation. UMI implementations will be developed and demonstrated in next-generation decision-support and autonomous systems. This program was previously funded in PE 0602702E, Project TT-13. ***FY 2017 Plans:*** - Formulate approaches for AI systems to explain their behavior and clarify the basis for and reliability of outputs. - Develop automated drill-down techniques that provide users with logic/data that drives AI system outputs/behaviors. - Develop a mathematically rigorous virtual stability theory for AI-enabled logic systems analogous to the (conventional) stability theory developed for dynamical systems. - Propose a general technology for building systems with the ability to understand, explain, and modify their behavior.	-	-	10.000
Accomplishments/Planned Programs Subtotals	48.636	60.948	56.039

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*

C. Other Program Funding Summary ($ in Millions)

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 2017 Defense Advanced Research Projects Agency			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
IT-05: *CYBER TECHNOLOGY*	-	63.891	39.664	0.000	-	0.000	0.000	0.000	0.000	0.000	-	-

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 2015	FY 2016	FY 2017
Title: Plan X	38.161	29.800	-

Description: The Plan X program is developing 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 is creating 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. Plan X funding continues in FY 2017 in Project IT-03.

FY 2015 Accomplishments:
- Created runtime environment and platforms capable of supporting a large scale user base, massive-scale deployments, resiliency to failure of any system component, and managed high ingest rates.
- Demonstrated military network tactical situational awareness applications and use cases.
- Released Plan X 1.0 system and field tested capabilities at Cyber Guard 2015.
- Conducted field tests of computer network operations scenario development and training capabilities.
- Planned transition to operational environments including understanding of transition partner networks and integration points.

FY 2016 Plans:
- Publish application store software development kit and integrate third party cyber capabilities.
- Refine analytics features for battlespace, analysis of courses of action, and planning subsystems.
- Adopt and integrate security access and use privileges, and demonstrate large-scale deployment of the end-to-end system with users in disparate locations.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Integrate with existing military command and control/intel systems to allow bidirectional flow of data to and from Plan X to provide visualization and insights into the cyber battlespace. - Release Plan X 2.0 system and field test capabilities at Cyber Flag 2016, and initiate technology transition with USCYBERCOM and Service components.			
Title: Cyber Grand Challenge (CGC) ***Description:*** The Cyber Grand Challenge (CGC) is creating 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. The CGC program is also funded in Project IT-03. ***FY 2015 Accomplishments:*** - Conducted mid-term qualification of finalist automated cyber technologies through competitive challenge. - Began second phase development of automated cyber defenders to allow real time in situ network defense decision-making. - Released first of two cyber research measurement and experimentation corpora with associated competition results. ***FY 2016 Plans:*** - Conduct world's first automated computer security contest: CGC Final Event. - Prepare automated systems for final competition via a multi-month series of audited trials. - Release final event results as cyber research corpus to measure and challenge future automated cyber capabilities.	16.832	9.864	-
Title: Crowd Sourced Formal Verification (CSFV) ***Description:*** The Crowd-Sourced Formal Verification (CSFV) program created 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 enabled non-specialists to participate productively in the formal verification process by transforming formal verification problems into user-driven simulations that are intuitively understandable. ***FY 2015 Accomplishments:*** - Completed development of five new simulations. - Refined simulations to make them accessible to a large set of non-specialists.	8.898	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Defense Advanced Research Projects Agency		Date: February 2016
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 2015	FY 2016	FY 2017
- Augmented simulations to handle large Java and C computer programs consisting of hundreds of thousands of lines of source code. - Enhanced public website to include these new simulations. - Assessed effectiveness of the new simulations on large-sized code targets.			
Accomplishments/Planned Programs Subtotals	63.891	39.664	-

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.

THIS PAGE INTENTIONALLY LEFT BLANK