Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Defense Advanced Research Projects Agency	Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
Total Program Element	-	331.720	353.635	392.784	-	392.784	380.359	389.940	384.550	380.931	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	34.233	42.459	49.919	-	49.919	59.775	52.113	70.413	70.413	-	-
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	209.557	255.137	260.757	-	260.757	235.669	248.985	234.201	222.597	-	-
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	46.508	56.039	82.108	-	82.108	84.915	88.842	79.936	87.921	-	-
IT-05: *CYBER TECHNOLOGY*	-	41.422	0.000	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 focuses on developing the computer hardware and associated software technologies required for future computationally- and data-intensive national security applications. Powerful new approaches are needed to manage the rapid growth in available sensor data, to leverage advances in machine learning and artificial intelligence, and to maintain the security of DoD information 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; to respond intelligently to new and unforeseen events; and to function not only as tools that facilitate human action but as partners to human operators. 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: FY 2018 Defense Advanced Research Projects Agency	Date: May 2017
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 developed 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 ensured DoD net-centric capabilities survive adversary cyber attacks and enabled new cyber-warfighting capabilities.

B. Program Change Summary ($ in Millions)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	341.358	353.635	353.925	-	353.925
Current President's Budget	331.720	353.635	392.784	-	392.784
Total Adjustments	-9.638	0.000	38.859	-	38.859
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	1.232	0.000			
• SBIR/STTR Transfer	-10.870	0.000			
• TotalOtherAdjustments	-	-	38.859	-	38.859

Change Summary Explanation

FY 2016: Decrease reflects the SBIR/STTR transfer offset by reprogrammings.

FY 2017: N/A

FY 2018: Increase reflects new start programs addressing machine learning technologies in the High Productivity, High Performance Responsive Architectures and Language Understanding and Symbiotic Automation projects.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	34.233	42.459	49.919	-	49.919	59.775	52.113	70.413	70.413	-	-

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project focuses on developing the computer hardware and associated software technologies required for future computationally- and data-intensive national security applications. Powerful new approaches are needed to manage the rapid growth in available sensor data, to leverage advances in machine learning and artificial intelligence, and to maintain the security of DoD information systems. The project therefore aims not only to create larger computing platforms but also to efficiently extract information out of large and chaotic data sets with embedded and low-size, weight, and power systems. Advances in these areas could allow DoD electronic systems to collaboratively manage scarce resources, such as the electromagnetic spectrum, and to adapt to new requirements and situations. Further, the resulting technologies, by being accessible to a wide range of application developers, should help develop new, sustainable computing systems for a broad spectrum of scientific and engineering applications.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Hierarchical Identify Verify Exploit (HIVE)*	4.000	16.709	19.919
Description: *Formerly Portable AnaLyticS (PALS) The Hierarchical Identify Verify Exploit (HIVE) program will pursue new hardware architectures and algorithms for rapidly integrating information from a variety of sources, increasing battlefield situational awareness. To develop operationally significant intelligence, human analysts today watch live battlefield feeds to detect items of interest, fusing together and interpreting information from multiple sensors and sources. The amount of information gathered, however, is quickly outstripping the human ability to review, process, fuse, and interpret. To resolve this challenge, HIVE seeks to leverage improvements in machine learning and artificial intelligence to augment the analyst's ability to integrate large streams of data. The program will investigate advances in chip architecture and data analytics algorithms that can allow machines to infer meaning out of data based on the information needs of the warfighter. Program success would therefore enable the warfighter to understand far more of the battlefield in real time. ***FY 2016 Accomplishments:*** - Identified common graph primitives that would accelerate the execution of DoD-specific applications.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Explored the applications benefitting from the unique architecture and whether unique hardware design allows for processors for unique military applications. ***FY 2017 Plans:*** - 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. - Prove, via simulation, improvement in the performance of core graph primitives including matrix indexing and assignment, matrix element-wise addition and multiplication, matrix - matrix products, and matrix scaling and reduction by 100X. - Develop graph application toolsets which take advantage of the new chip architectures. ***FY 2018 Plans:*** - Demonstrate the toolsets that can be applied to four different classes of DoD problems to include counter terrorism, cyber security, tactical decision making, and intelligence exploitation. - Demonstrate that these problems can run on prototype hardware systems and measure both power and performance improvements of the new hardware. - Use this information to create a chip design for future fabrication.			
Title: Electronic Globalization ***Description:*** The Electronic Globalization effort aims to develop advanced capabilities for validating the function of digital, analog, and mixed-signal integrated circuits (IC) given limited design specifications. These ICs are critical to nearly all military systems. Globalization and rapid growth in the commercial electronics industry have limited DoD's ability to influence and regulate IC fabrication. DoD today accounts for a relatively small portion of the overall IC market and the vast majority of IC manufacturing capacity lies overseas. As a result, parts acquired for DoD systems may not meet the stated specifications for performance and reliability. Electronic Globalization will pursue the technologies required to address this and other risks to DoD IC's, such as reverse engineering, counterfeiting, and the theft of U.S. intellectual property. The effort will support the development of key risk-reduction techniques including advanced imaging and computational methods for identifying an IC's functional elements. ***FY 2016 Accomplishments:*** - Improved the operation of a laser-based scanning tool to allow for its use in validating a wider array of microelectronic parts. - Demonstrated performance improvements on the order of 10x in the scanning tool, allowing for better accuracy in detecting counterfeit parts. ***FY 2017 Plans:*** - Study the effect of high stress on the reliability of conventionally fabricated commercial off the shelf (COTS) and Government off the shelf (GOTS) electronic components.	4.847	5.000	4.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Continue prototype system enhancements to the laser scanning tools. ***FY 2018 Plans:*** - Continue to study high stress effects on conventionally-fabricated COTS and GOTS electronic components.			
Title: Spectrum Collaboration Challenge (SC2)* ***Description:*** * Formerly Spectrum Grand Challenge The Spectrum Collaboration Challenge (SC2) program seeks to catalyze the development of systems, called Collaborative Intelligent Radios (CIRs) that intelligently share and optimize wireless spectrum usage without prior knowledge of each others' operating characteristics. SC2 will address the increasing demand for and reliance on unfettered wireless access. Today, assured access to the wireless spectrum involves restricting particular types of radios and radio operators to certain sets of fixed, pre-determined frequencies. Although this spectrum allocation approach helps ensure different radio signals do not interfere with each other, it is inherently inefficient and vulnerable to attack. First, allocated portions of the spectrum can remain unused or underutilized. Second, adversaries can easily characterize static spectrum allocations, identifying which ones to exploit or attack. SC2 will address this challenge by leveraging artificial intelligence and machine learning to optimize use of the spectrum in real-time. In particular, SC2 participants will be challenged to develop techniques that allow collaboration among dissimilar communications technologies. SC2 will conduct two preliminary competitions and one championship event over three years. The resulting technology will define a new class of radio systems that efficiently thrive in the absence of pre-planned spectrum. ***FY 2016 Accomplishments:*** - Defined SC2 rules governing eligibility as well how the competition will be conducted and scored and prizes ultimately awarded. - Identified a host and began development of the world's largest wireless environment emulator and research environment for the competition. - Announced the Spectrum Collaboration Challenge and stood up website to collect contact information. ***FY 2017 Plans:*** - Hold qualifying event for open participation in the first phase of the competition. - Select performers based on proposals for the competition's Proposal Track. - Complete design, build out and test of large-scale spectrum testbed. - Conduct competition scrimmages to allow competitor's to prepare for the Preliminary Event. ***FY 2018 Plans:*** - Hold preliminary competition, to take place on the custom-built competition testbed. - Hold second set of qualifying events to select additional Open Track participants.	5.000	14.750	18.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Develop visualizations and scoring for large-scale public event.			
Title: RF Machine Learning Systems (RFMLS) ***Description:*** The RF Machine Learning Systems (RFMLS) program will address the performance limitations of conventional radio frequency (RF) systems such as radar, signals intelligence, electronic warfare, or communications. Currently, the capabilities of these systems are fixed at the time of design and limited by their designer's vision. Conversely, a generic RFMLS system would learn how to reconfigure its circuits and processing to meet the requirements of a desired application in a specific environment. The relevant RF features are hand crafted and human specified today, and would instead be learned through machine learning algorithms applied within the RF system itself. The RFMLS system would later learn to adapt to changing conditions and requirements, making for a much more robust RF system solution. This flexibility should reduce the time and cost of continually re-designing and upgrading new systems and extend RF system performance beyond the limits of human designers. RMFLS exploits recent advancements in machine learning that have not previously been applied to RF systems. ***FY 2018 Plans:*** - Create datasets and infrastructure for use in training and evaluating RFML Systems. - Define a composable system architecture that enables multiple research teams to each confront a separate sub-system of the RF processing chain. - Quantify sub-system technology development requirements that support system performance goals by analyzing a variety of scenarios that are currently hand specified today. - Begin development of machine learning algorithms applied to the individual sub-system technologies.	-	-	8.000
Title: Cortical Processor* ***Description:*** *Formerly Complexity Management Hardware The Cortical Processor program aims to develop algorithms and hardware that can better handle the increasingly large and diverse sensor data streams used by battlefield systems. By leveraging advances in machine learning, the program could yield systems with the flexibility to understand and adapt to new contexts and new types of sensed data (e.g. new radio frequency or infrared signals). Current sensor platforms, conversely, are pre-programmed only to interpret specific data types and require a laborious coding effort to accommodate new types of data or contexts. Cortical Processor will develop hardware implementations that gracefully handle multiple data streams and limit the programming burden required for sensing and interpreting a complex scenario. The program will further be enabled by bio-inspired algorithms that benefit from research into biological learning and data processing. Cortical Processor's applied research component will investigate silicon circuit designs that are most suitable for high-performance, low-power, real-time sensing and data processing.	6.000	6.000	-

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
FY 2016 Accomplishments: - Benchmarked the accuracy of new bio-inspired machine learning features by performing a variety of recognition and control tasks. - Demonstrated the ability to manage multiple data streams with interlaced information. - Created high level hardware concepts for efficient machine learning using bio-inspired approaches. ***FY 2017 Plans:*** - Compare various bio-inspired algorithms' ability to extract complex information from feature-rich data sets. - Quantify the benefits of various architecture approaches to the management of large data streams when overlaid with contextual information. - Translate new algorithms to high level circuit implementations to show the power and processing requirements. - Fabricate bio-inspired machine learning chips capable of training and recognizing patterns in multiple, rich data streams.			
Title: Power Efficiency Revolution For Embedded Computing Technologies (PERFECT)	14.386	-	-
Description: The Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) program developed low-power, specialized, resilient data processing technologies to meet the requirements of next-generation Intelligence, Surveillance, and Reconnaissance (ISR) systems. Current embedded ISR applications rely on commercial processors designed for large data centers and therefore struggle to perform within the power and space limitations of platforms such as unmanned vehicles. As a result, these platforms often need to wirelessly access remote processing resources, potentially denying warfighters access to critical real-time information. Access to remote processing resources can also become unavailable in contested environments. To resolve this issue, PERFECT developed design tools and techniques to enable ISR sensor systems to process information locally, onboard the platform. These techniques should allow for processing data at lower voltages, speeding up data processing with specialized accelerators, and ensuring system reliability. ***FY 2016 Accomplishments:*** - Selected the implementation and transition target applications of vision, graph processing, and machine learning. Focused PERFECT teams' technologies to most effectively support future target application demonstrations. - Integrated modeling and evaluation environment, combining separate optimization tools for power, resiliency, and performance. - Demonstrated High Level Source-to-Source transformation targeting PERFECT program specialization simulators. Optimized/ vectorized code was generated that exploits explicit memory movement and dynamic voltage and frequency control for performance efficiency. - Demonstrated a near memory Fast Fourier transform accelerator supporting synthetic aperture radar and space-time adaptive processing using PERFECT architecture.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Demonstrated the benefits of specialization, using the PERFECT Vision Chip design as an example, by emulating the execution of major vision kernels to attain peak efficiencies.			
Accomplishments/Planned Programs Subtotals	34.233	42.459	49.919

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: FY 2018 Defense Advanced Research Projects Agency			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	209.557	255.137	260.757	-	260.757	235.669	248.985	234.201	222.597	-	-

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 enable the creation of secure, survivable, network-centric information systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	17.513	26.500	32.900

Description: The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is developing automated systems to detect attacks on critical U.S. electrical infrastructure, maintain situational awareness of the national power grid, and accelerate the recovery process in the event of an attack. The potential for a cyber-enabled attack on the U.S. power grid is a national security issue, as the ability of the military to deploy and project force is dependent on the effective and efficient functioning of civilian logistics and supply systems. RADICS will develop technologies to monitor heterogeneous distributed networks, detect anomalies that require rapid assessment, isolate compromised system elements, establish secure emergency communications networks, characterize attacks, and detect sensor spoofing. RADICS technology development is coordinated with and will transition to U.S. government elements responsible for defense of critical infrastructure.

FY 2016 Accomplishments:
- Explored design options for systems to detect anomalies in the physics of grid operation that may be indicative of the initial stages of a cyber attack.
- Studied options to enable network isolation of utilities under cyber attack, including the ad hoc formation of a secure emergency network using available communications links.
- Created initial designs of software tools to enable rapid localization and characterization of cyber attacks on the IT and Industrial Control Systems (ICS) networks of utilities.
- Conceptualized simulation-backed exercises to demonstrate the capabilities of tools and systems to potential transition partners.

FY 2017 Plans:
- Develop initial prototypes to detect anomalies in the physics of grid operation that may be indicative of the initial stages of a cyber attack.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Develop initial prototype tools to enable network isolation of utilities under cyber attack, including the ad hoc formation of a secure emergency network using available communications links. - Develop initial prototypes to enable rapid localization and characterization of cyber attacks on the IT and ICS networks of utilities. - Conduct the first simulation-backed exercise to assess the capabilities of tools and explore relevant concepts of operation for supporting the recovery of power in the aftermath of a large-scale outage due to cyber-enabled attack on the power grid. - Explore and design techniques to predict the nature and extent of cascading faults across large sections of a power grid. ***FY 2018 Plans:*** - Expand prototypes for grid physics anomaly detection, develop capability to detect attempts to spoof Supervisory Control and Data Acquisition (SCADA) telemetry, and incorporate techniques to predict cascading faults across large sections of a power grid. - Conduct large-scale network experiments to evaluate prototype techniques for forming secure emergency networks. - Expand prototypes for rapid localization and characterization of cyber attacks targeting ICS devices and networks to encompass a wider range of equipment and network protocols used in U.S. electrical infrastructure. - Conduct simulation-backed exercises to assess the capabilities of prototypes, explore relevant concepts of operation for supporting the recovery of power, and demonstrate the systems to potential transition partners. - Develop prototype capability to maintain and expand situational awareness in the aftermath of a cyber-enabled attack. - Explore and design techniques to monitor ICS networks for signs of cyber compromise during restart operations.			
Title: Extreme Distributed Denial of Service Defense (XD3) ***Description:*** The Extreme Distributed Denial of Service Defense (XD3) program is developing new computer networking architectures that 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 accelerate as the Internet of Things (IoT) incorporates new classes of devices that in many cases will be deployed with inadequate security controls: attackers will assimilate poorly defended IoT devices into 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 Accomplishments:*** - Explored alternative 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. - Proposed network maneuver and deception techniques that increase adversary work factors in target development, attack planning, and execution.	14.996	24.800	29.150

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Conceptualized the 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 attacks while preserving performance for legitimate users. ***FY 2017 Plans:*** - Develop network dispersion, maneuver, and adaptive response techniques that increase adversary work factors. - Develop testing capabilities to support iterative experimentation and demonstration of techniques. - Perform system-level demonstrations and subject systems to critical assessments to pinpoint design weaknesses and vulnerabilities. - Assess performance of developed systems with respect to program metrics including response time following attack, percentage recovery of application utility following attack, and application degradation in the absence of attack. ***FY 2018 Plans:*** - Implement and integrate network dispersion, maneuver, and adaptive response techniques in prototype systems that increase adversary work factors in target development, attack planning, and execution. - Perform final testing of dispersion, maneuver, and adaptive response with respect to program metrics. - Conduct military field exercises in collaboration with transition partners to elicit feedback on XD3 features, capabilities, and concepts of operation. - Incorporate feedback received during field exercises and re-test systems against program metrics to verify intended operation and desired transitionable features.			
Title: Leveraging the Analog Domain for Security (LADS)	17.000	20.500	23.000
Description: The Leveraging the Analog Domain for Security (LADS) program is developing 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 hidden. ***FY 2016 Accomplishments:*** - Formulated 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. - Investigated 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.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Proposed 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). - Develop statistical models for side channel emissions given imprecise/probabilistic knowledge of the executed code. ***FY 2018 Plans:*** - Implement an evaluation framework for Internet of Things (IoT) devices including instrumentation of the platforms, representative test software, program analysis and introspection. - Map selected features from the analog side channels to supervised models to confirm the software running on the device and its state, and identify deviations from the model due to specific attacker behaviors. - Demonstrate feasibility of discriminating between known/unknown code executing on a simple IoT-type device assuming knowledge of the firmware. - Evaluate and enhance the fidelity of the IoT monitor for the different IoT devices using the evaluation framework and explore performance tradeoffs including accuracy and sensor distance.			
Title: Brandeis ***Description:*** 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. Brandeis will break the tension between maintaining privacy and being able to tap into the huge value of data. 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 partners, and other stakeholders. Brandeis technologies are being designed to work with the virtualization, cloud computing, and software-defined networking technologies now widely used in both civilian and military environments. ***FY 2016 Accomplishments:*** - Implemented secure multiparty computation, secure database queries, differential privacy and remote attestation techniques in initial prototypes suitable for integration on commodity cloud infrastructures. - Developed a prototype evaluation platform and metrics/analysis tools on which privacy technologies can be tested and metrics computed.	17.600	19.000	22.300

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Initiated quantification of benefits of privacy technologies in the context of individual and enterprise use cases. ***FY 2017 Plans:*** - Optimize privacy prototypes that implement secure multiparty computation, secure database queries, differential privacy and remote attestation techniques, and test these prototypes 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. - Identify potential commercial and military transition partners for use of privacy technologies based on identified high priority use cases. ***FY 2018 Plans:*** - Develop and demonstrate a privacy-preserving information system using secure multiparty computation, secure database queries, differential privacy, and remote attestation techniques, in which individual and aggregate privacy desires can be easily understood and implemented consistently. - Demonstrate techniques for confirming that privacy preferences of data owners have been successfully received and honored. - Demonstrate privacy protection in human data communication and collaboration on enterprise networks.			
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. 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 exhibit differences in behavior under attack, so that CFAR-enabled computing systems will quickly detect deviations in processing elements at attack onset and rapidly reboot to restore affected services. CFAR technologies will be developed in coordination with operational users. ***FY 2016 Accomplishments:*** - Demonstrated replicated systems that exhibit sufficient variability to produce differences in behavior under attack. - Implemented and tested techniques for quickly detecting behavioral differences across replicated systems. - Evaluated multiple potential architectures for achieving cyber fault-tolerance for mission-critical systems running on commercial computing technologies. - Worked with potential transition partners to evaluate military computing systems as candidates for technology refresh with CFAR technologies. ***FY 2017 Plans:***	20.149	22.500	20.030

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Create replication variants from binary code to extend CFAR defenses to systems for which source code is not available. - Develop methods to produce proofs of semantic equivalence across variants, which will contribute to assurance cases that systems protected with CFAR technology behave identically to the original systems. - Develop robust cyber fault-tolerant models that handle the highly correlated and frequent faults that may result from a cyber-attack. - Experiment with an early CFAR prototype on a representative mission system. ***FY 2018 Plans:*** - Extend divergence proof system to reason about attacks and prove semantic equivalence of variants produced by the most effective diversity techniques. - Produce a scalable, efficient and potentially deployable capability that can protect a wide range of complex applications. - Refine and integrate test cases, instrumentation, data analysis repositories and tools to support independent evaluation of performance claims. - Develop technical documentation of design choices, data supporting the performance claims of components and the integrated CFAR system(s), and experimental results.			
Title: Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)	22.000	24.938	13.520
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 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 coordination with operational commands. ***FY 2016 Accomplishments:*** - Developed 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. - Demonstrated performance at the component and subsystem levels, to include real-time network analytics, holistic decision systems, and dynamically configurable protocol stacks. - Assessed EdgeCT component and system designs for potential weaknesses, vulnerabilities, and countermeasures associated with cyber attacks against network infrastructure, or against EdgeCT systems themselves.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Initiated development of software prototypes suitable for laboratory experimentation with operational commands. ***FY 2017 Plans:*** - Demonstrate and evaluate system prototypes against program metrics to verify adequate performance for cumulative network utility, recovery time, and network overhead. - 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. - Extend usage and testing scenarios to include multiple forms of simultaneous failures and cyber attacks within the wide area network. - Expose developed systems to red team analysis to identify potential operational vulnerabilities and focus further hardening of the technologies. ***FY 2018 Plans:*** - Foster transition activities through participation in a live military field exercise that will demonstrate EdgeCT capabilities in overcoming impairments to command and control (C2) and related networked applications. - Address and rectify operational vulnerabilities identified by red teams through additional design and testing activities within program testbeds. - Pursue transition to commercial network operators and to Defense Information Systems Agency through demonstrations and testing within service provider facilities, subjecting EdgeCT to impairments observed in network environments.			
Title: Dispersed Computing (DC) ***Description:*** The Dispersed Computing (DC) program will address research challenges encountered in the Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) program by developing techniques to distribute computing tasks across network computing elements to enable more efficient utilization of enterprise and Internet-based storage, processing, and networking resources. At present, enterprises and Internet-based IT service providers are increasingly adopting the cloud model, with data storage and computer processing concentrated in large data centers, which brings economies of scale and cost savings to storage and processing but creates problems for the network and for latency-sensitive applications due to the need to backhaul data to (often distant) data centers for processing. The DC program will develop a dispersed computing architecture that results in more efficient utilization of storage, processing, and networking resources. A key enabler for DC is the recent introduction by vendors of network elements that can be dual-purposed as computational elements. Under DC, these dual-purposed network-compute elements will be used to eliminate bottlenecks/chokepoints and mitigate impossible backhaul requirements by opportunistically moving code to data (and vice versa) given network conditions and available network-compute elements. With DC technology, the network becomes the cloud (and vice versa), and computation is performed where it is most efficient to do so.	-	13.000	17.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
FY 2017 Plans: - Devise data replication/decentralization strategies that enable local processing of data to greatly reduce loads on the network. - Explore the potential for adapting modern distributed computing paradigms such as MapReduce to run on dispersed DC-enabled network-compute elements and virtual computing clusters. - Design protocols that enable the DC architecture to run reliably and efficiently on tactical networks that exhibit disruptions, intermittent connectivity, and low bandwidth. ***FY 2018 Plans:*** - Complete initial prototypes of programmable protocol stacks operating on network-compute elements to boost network transport of code and data and to demonstrate the tailoring of protocols to the needs of specific military applications such as command and control (C2) and querying of distributed data stores. - Establish and validate testbeds and instrumentation that enable reliable measurement of program metrics, such as network load reduction and operational scale. - Complete initial prototypes of software control systems to govern access to dispersed network-compute elements and conduct initial demonstrations of these prototypes to Defense Information Systems Agency, combatant commands, or other DoD stakeholders.			
Title: Supply Chain Hardware Integrity for Electronics Defense (SHIELD)	21.000	18.000	6.000
Description: The Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program aims to develop a technology capable of confirming the authenticity of electronic parts at any time and place. Authenticating parts or detecting counterfeit components by current means has proven expensive, time-consuming, and of limited effectiveness. An alternative solution, maintaining complete control of the global supply chain using administrative controls, can also incur substantial costs. SHIELD instead seeks to incorporate a small, inexpensive silicon chip ("dielet") into the packaging of genuine components. The dielet would provide unique and encrypted component identification, enabling authentication from very close proximity. Since counterfeit electronic components pose a threat to the integrity and reliability of both commercial and DoD systems, SHIELD would fulfill a large, pressing, and evolving need for anti-counterfeit technologies. ***FY 2016 Accomplishments:*** - Refined designs based on measured results from test site hardware. - Developed transaction model for reader-to-dielet interrogation. - Selected best-fit Phase 1 technologies for inclusion on Phase 2 dielet designs, based on validated hardware measurements and objective analysis of design compatibility. - Refined dielet singulation, test and insertion methodology and fragility design based on mechanical testing of surrogate dielets. ***FY 2017 Plans:***			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Design and manufacture prototype SHIELD dielets, integrating best-fit technologies selected during Phase 1. - Develop hardware demonstration vehicle to evaluate Phase 1 power and sensor technologies in 65 nanometer complementary metal-oxide-semiconductor (CMOS). - 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 testing. ***FY 2018 Plans:*** - Demonstrate the SHIELD concept of operation in an actual or environmental facsimile of an integrated circuit supply chain. - Incorporate SHIELD dielets into IC packaging and test with a server-connected reader device at various points in the supply chain. - Perform environmental stress and reliability testing on parts with embedded SHIELD dielets to demonstrate that the dielet insertion has no adverse impact on the host IC's performance or reliability.			
Title: Enhanced Attribution ***Description:*** The Enhanced Attribution program, building upon the Active Cyber Defense program, will develop technologies to associate the malicious actions of cyber adversaries to individual cyber operators and then to enable the government to reveal publicly the malicious actions of individual cyber operators without damaging sources and methods. Technologies of interest include new approaches for identification of malicious cyber operators, techniques to deconstruct their software tools and actions into semantically rich and compressed knowledge representations, algorithms for developing predictive behavioral characteristics, and methods for confirming this information with other commercial and public sources of data. As Enhanced Attribution technologies mature and show promise they will be implemented in tools for evaluation by potential transition sponsors. ***FY 2016 Accomplishments:*** - Formulated approaches for associating malicious actions with individual cyber operators. - Developed a concept for public attribution without revealing sources and methods. - Identified initial open source and commercially available data sources that can be used to confirm a cyber operations model. ***FY 2017 Plans:*** - Develop an ontology of cyber operator actions and identify useful metadata. - Develop and apply flexible database technology to support storage and causal relationship identification of operational cyber data. - Develop initial attribution modules to summarize behavioral characteristics for at least two computing platforms. - Conduct an initial adversarial evaluation against a simulated threat to provide feedback and drive future development goals.	8.000	17.500	23.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Develop automated techniques to detect phishing attacks and to defeat adversary social engineering activities before they can extract sensitive information from vulnerable individuals. ***FY 2018 Plans:*** - Reduce computational and bandwidth requirements for attribution modules. - Connect the basic attribution technologies and demonstrate the capability to generate narrative descriptions of cyber operator activities. - Demonstrate anticipatory analytics for adversary cyber operator actions. - Conduct an adversarial evaluation against a simulated threat in collaboration with transition partner operators.			
Title: System Security Integrated Through Hardware and software (SSITH) ***Description:*** The System Security Integrated Through Hardware and Software (SSITH) program seeks to secure DoD and commercial electronic systems against cybersecurity threats by developing novel hardware/firmware security architectures and hardware design methodologies. Current responses to cybersecurity attacks typically consist of developing and deploying software patches to address specific vulnerabilities in a software firewall without addressing potential vulnerabilities in the underlying hardware architecture. To address this challenge, SSITH will drive new research in electronics hardware security and exploit current research in areas such as cryptographic-based computing and hardware verification. Implementation of these advanced ideas has been enabled by the extremely capable semiconductor technology driven by Moore's Law. The program will also investigate flexible hardware architectures that adapt to and limit the impact of new cybersecurity attacks. Finally, SSITH will seek to mitigate the potential negative impact of new security protection architectures on system performance and power usage. Once developed, SSITH capabilities will be applicable to both commercial and military electronic systems. ***FY 2017 Plans:*** - Define new hardware architectures that implement scalable, flexible, and robust protection against external attacks on hardware. - Utilize modeling and simulation approaches to determine the expected improvement in protection of the new hardware architectures relative to current software only protection. - Establish initial system security metrics and hardware security representations to system security systems. ***FY 2018 Plans:*** - Implement new hardware architectures that demonstrate scalable, flexible, and robust protection against external attacks on hardware. - Utilize simulation and hardware emulation to confirm the expected improvement in protection of the new hardware architectures relative to current software only protection.	-	12.000	19.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Evaluate SSITH security approaches through independent Red Team attack on the security architectures as implemented in hardware. - Define and start full system hardware demonstrations of security architectures.			
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 Project IT-03 for testing, evaluation and optimization through participation in tactical level exercises and for integrating Plan X technologies into transition partner systems. ***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 Army Warfighting Assessment (AWA), Cyber Guard, Cyber Flag, and Red Flag. - Refine operator workflows and operational use cases based on feedback gathered during exercises and user studies. ***FY 2018 Plans:*** - Work with transition partners, such as U.S. Cyber Command (USCYBERCOM), U.S. Army Cyber Command (ARCYBER), and U.S. Army Program Executive Office Enterprise Information Systems (PEO EIS) to integrate Plan X into transition partner systems.	-	23.349	7.546
Title: Cyber Assured Systems Engineering (CASE) ***Description:*** The Cyber Assured Systems Engineering (CASE) program aims to enable the systematic design of networked cyber physical systems to be resilient against cyberattacks. The current state-of-practice for cyber resilience utilizes penetration testing after system construction to drive post-design re-engineering. The CASE technical approach is to formulate cyber resilience as an explicitly engineered property, similar to other holistic properties such as safety, durability, and reliability now standard in systems engineering. CASE will focus on the following technical areas: techniques to derive resilience-related requirements before system design and construction; architectural design and analysis tools to design-in the derived resilience requirements while providing feedback to the human designer to allow for informed tradeoffs between resilience and other system design goals; tools to adapt existing software to support system-level resilience requirements; and inference engines, satisfiability solvers, and	-	-	17.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
provers scalable to complex networked cyber physical systems. If successful, CASE technologies will enable the design of cyber physical systems that robustly execute their intended function despite the efforts of sophisticated cyber adversaries. CASE builds on technology developed in the High Assurance Cyber Military Systems program. ***FY 2018 Plans:*** - Develop techniques to derive resilience-related requirements before system design and construction. - Develop architectural design and analysis tools to design-in derived resilience requirements while providing feedback to the human designer to allow for sensible tradeoffs between resilience and other system design goals. - Formulate cyber resilience design challenge problems relevant to military cyber physical systems. - Explore the potential for using formal methods to enable secure network interactions. - Create tools to adapt existing software to support system-level resilience requirements and inference engines, satisfiability solvers, and provers scalable to complex cyber physical systems. - Develop techniques for translating the output of cyber resilience design tools into concepts relevant to the system designer. - Demonstrate and evaluate design tools and techniques on an initial cyber resilience design challenge problem. - Initiate development of provably secure, maintainable open source versions of fully-featured, highly-performance, network infrastructure.			
Title: Automated Cyber Operations and Defense (ACOD)	-	-	12.257
Description: The Automated Cyber Operations and Defense (ACOD) program will develop a semi-automated cyber operations system to enable operators to detect and respond to cyber attacks more rapidly than unaided human operators. The ACOD 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. As with algorithmic trading of financial instruments, the program envisions high-intensity cyber operations conducted by computers under human supervision. To accomplish this, ACOD will combine automated cyber defense capabilities, such as those developed in DARPA's Cyber Grand Challenge, with human-centric cyber operations planning and execution capabilities, such as those developed under DARPA's Plan X program. Through human-machine cyber teaming, ACOD will ensure U.S. operational superiority across the spectrum of cyber conflict. ***FY 2018 Plans:*** - Explore techniques for assessing the presence and seriousness of cyber vulnerabilities in new or existing software systems, enterprise networks and server configurations. - Develop concepts of operations for mixed-initiative cyber operations. - Design a cyber operations reasoning framework that a machine can use to determine which possible actions are allowable under rules of engagement; to rank alternative allowable actions in terms of likely efficacy; and to decide when an action may proceed.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Propose interface strategies that facilitate timely human understanding of rapid changes in the cyber battlespace and effective human interaction with computerized cyber defenders. - Identify and tailor automation modes appropriate for use across the cyber conflict spectrum.			
Title: Cyber-Hunting at Scale (CHASE) ***Description:*** The Cyber-Hunting at Scale (CHASE) program will develop data-driven tools for real-time cyber threat detection, characterization, and protection within enterprise-scale networks. U.S. computer networks are continually under attack, but at present no tools exist to efficiently extract the right data from the right device at the right time to analyze these attacks. The nature of the threat should be used to determine which data and analyses are required. For example, analysis of an in-memory exploit would require detailed data from a few devices, while analysis of a global botnet attack would require summary data from millions of devices. CHASE is will develop novel algorithms and analysis tools to dynamically collect data from across the network, actively hunt for advanced threats that evade routine security measures, and disseminate protective measures that automatically bolster the collective cyber defense posture. ***FY 2018 Plans:*** - Devise algorithms to process raw and summary cyber data and construct feature sets for indicators of adversary activity. - Formulate mathematical approaches for developing data collection, transmission and retention policies. - Develop initial distributed algorithms to enhance enterprise-scale cyber situational awareness.	-	-	18.054
Title: High Assurance Cyber Military Systems ***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 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. Additionally, the program will explore the use of formal methods to bring high levels of inherent assurance to Internet-enabled applications, in particular, applications involving remote update, access, management, authorization, and control. ***FY 2016 Accomplishments:***	20.475	12.974	-

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Applied an architecture-based approach to high-assurance system development, enabling an effective cyber retrofit for a number of vehicles including a military helicopter and a military transport vehicle. - Demonstrated machine-tracked assurance cases for system-wide security properties on targeted vehicles, and increased the level of automation of proof generation in theorem provers. - Demonstrated the effectiveness of approaches by conducting penetration-testing exercises on the targeted vehicles. ***FY 2017 Plans:*** - Formulate assurance cases for complex mission critical systems that are comprised of multiple interacting components.			
Title: Vetting Commodity Computing Systems for the DoD (VET) ***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 cyber attack. ***FY 2016 Accomplishments:*** - Measured 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. - Conducted an integrated end-to-end software/firmware-vetting technology demonstration relevant to potential transition partners. - Initiated an effort to apply VET technologies to naval industrial control environments. ***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.	22.625	13.520	-
Title: Cyber Grand Challenge (CGC) ***Description:*** The Cyber Grand Challenge (CGC) program 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,	11.329	6.556	-

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
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 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 2016 Accomplishments:*** - Prepared automated systems for final competition via a multi-month series of audited trials. - Conducted world's first automated computer security contest: Cyber Grand Challenge Final Event. - Released event results as cyber research corpus to measure and challenge future automated cyber capabilities. ***FY 2017 Plans:*** - Capture the lessons learned from the Cyber Grand Challenge Final Event to inform the design of future automated systems capable of engaging human experts. - Benchmark and baseline the abilities of expert reverse engineers to guide the creation of a machine-vs-expert evaluation corpus. - Formulate an infrastructure that allows for distributed machine-vs-expert engagements.			
Title: Active Cyber Defense (ACD) ***Description:*** The Active Cyber Defense (ACD) program developed technologies to enable DoD cyber operators to leverage 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 developed 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 2016 Accomplishments:*** - Completed integration of system platforms and demonstrated capabilities to transition partners. - Performed final test and evaluation of integrated capabilities and secured partners for operational deployment. - Supported efforts to deploy capability to DoD and other U.S. Government cyber operators.	6.270	-	-
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	6.100	-	-

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
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 eliminated known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH also developed software techniques that allowed a computer system to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH developed techniques to make each computer system appear unique to the attacker and allow each system to change over time. ***FY 2016 Accomplishments:*** - Transitioned symbiotes capability (secure code structures embedded in device firmware that can provide a variety of cyber defense functions) to Air Force and Navy. - Transitioned microprocessor instruction set architecture security extensions to commercial processor designer.			
Title: Mission-oriented Resilient Clouds (MRC) ***Description:*** The Mission-oriented Resilient Clouds (MRC) program created 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 addressed this risk by creating advanced network protocols and new approaches to computing in potentially compromised distributed environments. Attention focused on adapting defenses and allocating resources dynamically in response to attacks and compromises. MRC resulted in new approaches to measure trust, reach consensus in compromised environments, and allocate resources in response to current threats and computational requirements. MRC developed new verification and control techniques for networks embedded in clouds that must function reliably in complex adversarial environments. ***FY 2016 Accomplishments:*** - Collaborated with Defense Information Systems Agency in evaluating prioritized- and guaranteed-delivery enhancements to commercial networking technologies. - Collaborated with Naval Sea Systems Command on techniques to authenticate multicast packets on networked cyber physical systems on ships.	4.500	-	-
Accomplishments/Planned Programs Subtotals	209.557	255.137	260.757

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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*

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: FY 2018 Defense Advanced Research Projects Agency			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	46.508	56.039	82.108	-	82.108	84.915	88.842	79.936	87.921	-	-

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; to respond intelligently to new and unforeseen events; and to function not only as tools that facilitate human action but as partners to human operators. 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. The technologies developed in this project will be applied to intelligence analysis, command and control, cyberspace operations, electronic warfare, and robotics.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Low Resource Languages for Emergent Incidents (LORELEI)	22.225	25.907	31.574
Description: The Low Resource Languages for Emergent Incidents (LORELEI) program is developing technology to rapidly field machine translation and other language processing capabilities for low-resource foreign languages. The U.S. 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. Processing foreign language materials requires 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 takes 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 2016 Accomplishments: - Developed initial techniques for quantifying the linguistic similarity of language usage in diverse documents and media. - Developed initial algorithms to exploit the universal properties of languages when rapidly ramping up for a low-resource language. - Developed semantic techniques for identifying the common topics, themes, and sentiment in speech and text in diverse foreign languages.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Collected, generated, and annotated data for an initial set of resources in typologically representative medium-resource languages. - Created 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 new languages and measure progress on the languages evaluated in the previous year. ***FY 2018 Plans:*** - Extend development of means to determine opinions and beliefs in low-resource languages in speech signals as well as text. - Integrate multiple new algorithms for low-resource language analysis with a graphical user interface and evaluate the interface platform with end users. - Evaluate the performance of the analysis algorithms on new languages and measure progress on the languages evaluated in the previous year.			
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 specific foreign languages, and sources may be reports, messages, or other documents. DEFT will extract knowledge at scale for open source intelligence and threat analysis. Transition partners include the intelligence community and operational commands. ***FY 2016 Accomplishments:*** - Improved algorithm performance on current functions and extended single-document algorithms to function across multiple documents. - Merged and optimized combined output of algorithms focused on different tasks such as belief and sentiment extraction, event argument and attribute identification, and relation mapping.	18.762	13.632	9.394

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Developed methods for evaluating the effectiveness of various natural language processing algorithms in a multi-lingual environment, including evaluation of sentiment and belief analysis. - Transitioned additional component prototypes to end-user sites for effectiveness assessment. ***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. ***FY 2018 Plans:*** - Develop techniques to integrate diverse information from multiple intelligence sources into a uniform schema amenable to machine reasoning and human collaboration. - Develop reasoning strategies capable of identifying information gaps, reconciling conflicting information, and proposing the most likely completions for partially specified knowledge. - Optimize techniques and prototypes based on feedback from operational users.			
Title: Explainable Artificial Intelligence (XAI)* ***Description:*** *Previously Understanding Machine Intelligence (UMI) The Explainable Artificial Intelligence (XAI) program is developing a new generation of machine learning techniques that are able to produce a rationale to explain the conclusions they reach. If current trends continue, future U.S. military autonomous systems will need to perform increasingly complex and sensitive missions, and AI will be critical to such systems. However, in order for developers, users, and senior leaders to feel confident enough to deploy and use AI-enabled systems, these systems must be able to explain their rationale, and their recommendations, decisions, and actions must be delivered in a way that military users can understand and trust. Today most machine learning systems provide no explanations or provide explanations that are too detailed, at the wrong level of abstraction, or not meaningful to a human user. XAI will develop the tools necessary to build explainable AI systems, in particular (1) new machine learning techniques that produce human-interpretable models and (2) user interfaces that generate explanations from those models meaningful to end-users. XAI implementations will be developed and demonstrated in next-generation autonomous and decision-support systems. ***FY 2017 Plans:*** - Formulate approaches for AI systems to explain their behavior and clarify the basis for and reliability of outputs. - Propose a general interface technology that communicates the internals of machine learning models in a human-interpretable fashion.	-	11.000	23.840

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Explore designs for a complete explainable AI system that consists of explainable machine learning models and an explanation generation interface. - Explore approaches for autonomous planning and execution of tasks based on high level goals and constraints. ***FY 2018 Plans:*** - Develop and demonstrate an initial prototype of an explainable AI system using modified deep learning techniques to produce deep neural nets that are more interpretable than current techniques. - Develop and demonstrate an initial prototype of an explainable AI system using structured, causal machine learning techniques that are inherently more interpretable. - Develop and demonstrate an initial prototype of a system that creates an explainable model for an existing black box machine learning system. - Integrate artificial intelligence and robust control techniques to ensure predictable and trustable autonomous operations in uncertain and adversarial environments. - Formulate perceptually-grounded representations to enable commonsense reasoning by machines about the physical world and spatio-temporal phenomena. - Explore quantitative approaches for creating human-computer teams through the inclusion of individuals and computers/ autonomous systems with complementary characteristics/capabilities.			
Title: Active Interpretation of Disparate Alternatives (AIDA) ***Description:*** The Active Interpretation of Disparate Alternatives (AIDA) program is developing a multi-hypothesis semantic engine that generates explicit alternative interpretations of events, situations, and trends from a variety of unstructured sources, for use in an environment where there are noisy, conflicting, and potentially deceptive data. Information from each medium is often analyzed independently, without the context provided by information from other media resulting in only one interpretation, with alternatives being eliminated due to lack of evidence even in the absence of contradictory evidence. When these independent, impoverished analyses are combined, generally late in the analysis process, the result can be a single apparent consensus view that does not reflect a true consensus. To overcome these limitations, AIDA seeks to research, develop, and demonstrate technology capable of automatically mapping information derived from multiple sources into a common semantic representation, aggregating information, resolving ambiguities, discovering conflicting information, and generating and exploring multiple interpretations of events, situations, or trends of interest. If successful, AIDA will provide decision makers a capability to understand alternatives and make contingency plans accordingly. Transition partners include operational commands and the intelligence community. AIDA builds on technology developed in the Deep Exploration and Filtering of Text program. ***FY 2017 Plans:*** - Develop an initial semantic representation language for a common semantic representation from diverse sources.	-	5.500	17.300

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
- Adapt multimedia-analysis algorithms to produce information suitable for use in a common semantic representation and to accept and utilize information from the common semantic representation or from the generated interpretations. - Explore semantic techniques that automatically generate, update, rank, and prune alternative interpretations as they become more or less likely given incoming data streams. ***FY 2018 Plans:*** - Develop techniques to integrate diverse information from multiple sources into a uniform schema amenable to machine reasoning and human collaboration. - Develop techniques to extend known ontologies using information from diverse sources. - Develop techniques to estimate the confidence of the generated interpretations considering accuracy of the analysis, provenance, and source veracity. - Develop techniques to quantify the possibility that an interpretation is based on semantically consistent misinformation injected by an adversary.			
Title: Robust Automatic Transcription of Speech (RATS) ***Description:*** The Robust Automatic Transcription of Speech (RATS) program developed 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 were developed for speech activity detection, language identification, speaker identification, and keyword spotting. RATS technology was optimized on real world data in conjunction with several operational users. ***FY 2016 Accomplishments:*** - Developed, integrated and tested techniques to deal with multiple speakers and overlapping speaker channels. - Developed unified Application Programming Interface to support multiple tactical integration platforms. - Integrated technologies into multiple transition partner platforms and operations.	5.521	-	-
Accomplishments/Planned Programs Subtotals	46.508	56.039	82.108

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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*

E. Performance Metrics

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

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
IT-05: *CYBER TECHNOLOGY*	-	41.422	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	-	-

A. Mission Description and Budget Item Justification

The Cyber Technology project developed 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 ensured 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 2016	FY 2017	FY 2018
Title: Plan X	32.362	-	-
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 2016 Accomplishments:*** - Published application store software development kit and integrated third party cyber capabilities. - Refined analytics features for battlespace, courses of action analysis, and planning subsystems. - Adopted and integrated security access and use privileges, and demonstrated large-scale deployment of the end-to-end system with users in disparate locations. - Integrated with existing military cyber threat/intel systems to allow bidirectional flow of data to and from Plan X to provide visualization and insights into the cyber battlespace. - Released Plan X 2.0 system and field tested capabilities at Cyber Guard/Cyber Flag 2016, and initiated technology transition with U.S. Army Cyber Command (ARCYBER) and U.S. Army Program Executive Office, Enterprise Information Systems (PEO EIS).			
Title: Cyber Grand Challenge (CGC)	9.060	-	-
Description: The Cyber Grand Challenge (CGC) program 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,			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Defense Advanced Research Projects Agency		Date: May 2017
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 2016	FY 2017	FY 2018
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 2016 Accomplishments:*** - Prepared automated systems for final competition via a multi-month series of audited trials. - Conducted world's first automated computer security contest: Cyber Grand Challenge Final Event. - Released final event results as cyber research corpus to measure and challenge future automated cyber capabilities.			
Accomplishments/Planned Programs Subtotals	41.422	-	-

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.