Exhibit R-2, **RDT&E Budget Item Justification:** PB 2019 Defense Advanced Research Projects Agency	**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
Total Program Element	-	341.942	392.784	395.317	-	395.317	376.946	392.956	409.437	404.937	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	42.442	49.919	55.885	-	55.885	48.613	69.313	80.413	80.413	-	-
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	243.642	260.757	259.359	-	259.359	237.491	241.707	239.103	234.603	-	-
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	55.858	82.108	80.073	-	80.073	90.842	81.936	89.921	89.921	-	-

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 while under attack, and to be rapidly recovered/reconstituted in the aftermath of an 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:** PB 2019 Defense Advanced Research Projects Agency	**Date:** February 2018
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* I BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602303E I *INFORMATION & COMMUNICATIONS TECHNOLOGY*

B. Program Change Summary ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**
Previous President's Budget	353.635	392.784	380.359	-	380.359
Current President's Budget	341.942	392.784	395.317	-	395.317
Total Adjustments	-11.693	0.000	14.958	-	14.958
• 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	3.100	0.000			
• SBIR/STTR Transfer	-14.793	0.000			
• TotalOtherAdjustments	-	-	14.958	-	14.958

Change Summary Explanation

FY 2017: Decrease reflects the SBIR/STTR transfer offset by reprogrammings.
FY 2018: N/A
FY 2019: Increase reflects new start programs addressing artificial intelligence and human-machine collaboration in the Information Assurance and Survivability and Language Understanding and Symbiotic Automation projects.

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	42.442	49.919	55.885	-	55.885	48.613	69.313	80.413	80.413	-	-

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 2017	FY 2018	FY 2019
Title: Spectrum Collaboration Challenge (SC2) ***Description:*** 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 other's 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 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.	14.750	18.000	23.885

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
- Develop visualizations and scoring for large-scale public event. ***FY 2019 Plans:*** - Hold second competition, to take place on the custom-built competition testbed. - Hold third set of qualifying events to select additional Open Track participants. - Develop final competition event execution plan. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase in FY 2019 reflects preparation for final competition.			
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 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. - Begin development of machine learning algorithms and architectures applied to four different challenge problems. - Evaluate integratability of machine learning algorithms and architectures with candidate RF hardware systems. - Identify existing DoD RF systems to upgrade with RFMLS machine learning. ***FY 2019 Plans:*** - Complete development of machine learning algorithms and architectures for two of four challenge problems. - Test preliminary performance of solutions for all four challenge problems and complete final testing for two challenge problem solutions. - Begin development of an RF hardware system to host field testing and demonstrations. ***FY 2018 to FY 2019 Increase/Decrease Statement:***	-	10.000	23.000

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
The increase in FY 2019 reflects completing the development of machine learning algorithms and beginning the process of demonstrating machine learning algorithms on a test platform.			
Title: Adversarial AI for RF ***Description:*** The Adversarial AI for RF program aims to develop artificial intelligence (AI) capabilities with applications for national security, particularly in areas such as electronic warfare. Given that U.S. and potential adversaries are developing AI technology with potentially revolutionary capabilities, DoD must prepare for conflicts that include offensive and defensive AI actors. Adversarial AI will develop methodologies for protecting AI-enabled DoD systems from adversary attempts to elicit an erroneous response (spoofing) and for significantly increasing AI system reliability and safety. The resulting AI algorithms should also ensure that AI-enabled DoD devices offer human-understandable explanations for their suggested course of action, to the maximum extent possible. To enable this future, the Adversarial AI program will leverage and advance newly formed links between machine learning and security and look to extend these emerging techniques to military specific domains that are emerging such as cognitive Electronic Warfare (EW) systems. Finally, the program may inform the correct mechanism to train AI systems for use in adversarial situations. ***FY 2019 Plans:*** - Specify and bound problem domains, selecting those where the program will have the greatest impact. - Develop new theoretical and algorithmic foundations of lifelong learning cryptographic and waveform attacks and defense. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase in FY 2019 reflects program initiation.	-	-	9.000
Title: Hierarchical Identify Verify Exploit (HIVE) ***Description:*** 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 2018 Plans:***	16.692	19.919	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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*

<u>B. Accomplishments/Planned Programs ($ in Millions)</u>	**FY 2017**	**FY 2018**	**FY 2019**
- Demonstrate that the toolsets can be applied to four different classes of DoD problems to include counter terrorism, cyber security, tactical decision making, and intelligence exploitation. - Demonstrate these problems can run on a field programmable gate array which emulate the HIVE chip and measure both power and performance improvements of the proposed design architectures. - Use this information to create a chip design for future fabrication. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The decrease in FY 2019 reflects the program moving to PE 0602716E/ Project ELT-02.			
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 2018 Plans:*** - Continue to study high stress effects on conventionally-fabricated commercial off the shelf (COTS) and government off the shelf (GOTS) electronic components. - Finalize and test models of high stress effects on conventionally-fabricated parts to verify accuracy and tolerances of models. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The decrease in FY 2019 reflects program completion.	5.000	2.000	-
Title: Cortical Processor ***Description:*** The Cortical Processor program developed 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 yielded 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 developed hardware implementations that gracefully handle multiple data streams and limit the programming burden required for sensing and interpreting a complex	6.000	-	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
scenario. The program was enabled by bio-inspired algorithms that benefit from research into biological learning and data processing. Cortical Processor's applied research component investigated silicon circuit designs that are most suitable for high-performance, low-power, real-time sensing and data processing.			
Accomplishments/Planned Programs Subtotals	42.442	49.919	55.885

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

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

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	243.642	260.757	259.359	-	259.359	237.491	241.707	239.103	234.603	-	-

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)

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	26.500	30.900	34.000

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 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 industrial control system (ICS) devices and networks to encompass a wider range of equipment and network protocols used in U.S. electrical infrastructure.
- Develop prototype capability to maintain and expand situational awareness in the aftermath of a cyber-enabled attack on the power grid.
- Explore and design techniques to monitor ICS networks for signs of cyber compromise during restart operations.

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**

- Conduct simulation-backed exercises to assess the capabilities of prototypes, explore relevant concepts of operation for supporting the recovery of power, and provide potential transition partners with the opportunity to guide prototype refinement.

FY 2019 Plans:
- Develop robust capability for grid physics anomaly and SCADA-spoofing detection, and incorporate methods for detecting downstream disturbances caused by malicious manipulations of the bulk power markets.
- Develop approaches to augment and optimize the use of available communications links to create ad hoc secure emergency communications networks under conditions of substantial uncertainty.
- Develop capability for rapid localization and characterization of cyber weapons targeting a wide range of ICS devices and networks, and develop automated approaches to support cyber first responders in remediation efforts.
- Demonstrate capabilities to maintain and expand situational awareness in the aftermath of a cyber-enabled attack on the power grid.
- Conduct simulation-backed exercises to evaluate readiness for transition of RADICS tools, engage with potential transition partner personnel to enable them to use the tools in these exercises, and gather feedback on tool effectiveness.

FY 2018 to FY 2019 Increase/Decrease Statement:
The FY 2019 increase reflects continued development of technologies for rapid recovery of the power grid from a cyber attack and expanded simulation-backed exercises to establish readiness for transition.

Title: Dispersed Computing	13.000	17.000	21.800

Description: The Dispersed Computing program is 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 Information Technology (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 Dispersed Computing program will develop a dispersed computing architecture that results in more efficient utilization of storage, processing, and networking resources. A key enabler is the recent introduction by vendors of network elements that can be dual-purposed as computational elements. These dual-purposed network-compute elements will be used to eliminate bottlenecks/chokepoints, and mitigate impossible backhaul requirements by opportunistically moving code to data given network conditions and available network-compute elements. With Dispersed Computing technology, the network becomes the cloud and computation is performed where it is most efficient to do so.

FY 2018 Plans:

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
- Complete initial prototypes of programmable protocol stacks operating on network-compute elements to boost network transport of code and data. - Tailor protocols to the needs of specific military applications, such as command and control 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 (DISA) and their commercial network providers. ***FY 2019 Plans:*** - Incorporate feedback received from demonstrations to refine network-compute element use cases and metrics. - Implement integrated prototype network-compute elements that incorporate dispersed computation algorithms and programmable protocol stack functionality. - Demonstrate and evaluate integrated prototype network-compute elements against program metrics. - Demonstrate integrated network-compute element prototypes to DISA and their commercial network providers. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase reflects continued development of the technologies and software prototypes required to distribute workloads to network-compute elements and expanded demonstrations for potential transition partners.			
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 resolve 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 controlled 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 2018 Plans:*** - Develop and demonstrate privacy-preserving information systems using secure multiparty computation, secure database queries, differential privacy, and remote attestation techniques, in which individual and aggregate privacy objectives can be easily understood and implemented consistently. - Demonstrate techniques for confirming that privacy preferences of data owners have been successfully received and honored.	16.000	17.000	20.750

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
- Work with U.S. government and DoD stakeholders to develop demonstration efforts for privacy-preserving technologies on operational systems. ***FY 2019 Plans:*** - Scale up secure multiparty computation, secure database queries, differential privacy, and remote attestation techniques to U.S. government and DoD data repositories. - Participate in real-world exercises that demonstrate privacy protection in data communication and collaboration on enterprise networks. - Incorporate privacy-preserving technologies in flexible toolkits and transition to U.S. government and DoD transition partners. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of Brandeis development work continuing and the expansion of efforts to demonstrate technologies on U.S. government and DoD use cases.			
Title: Leveraging the Analog Domain for Security (LADS) ***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 2018 Plans:*** - Implement an evaluation framework for Internet of Things (IoT) devices including instrumentation of the platforms and representative test software. - Map selected features from the analog side channels to statistical 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 different IoT devices using the evaluation framework, and explore performance tradeoffs including accuracy and sensor distance. ***FY 2019 Plans:*** - Design antenna arrays and develop signal pre-processing techniques to improve signal-to-noise properties and enable higher-fidelity device monitoring from longer distances against both IoT devices and more complex devices such as thin-clients, feature phones, smart phones, laptops, and servers.	20.500	19.700	15.300

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
- Characterize and model the signals from thin-client, feature phone, smart phone, laptop, and server devices operating in secure/correct and compromised/faulty states. - Refine side channel models and use them to guide the development of software-based signal boosting techniques. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease is the result of development work maturing and the focus shifting to optimization of techniques for use in operational environments.			
Title: Extreme Distributed Denial of Service Defense (XD3)	22.800	26.000	12.500
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 both high-volume flooding attacks and more subtle low-volume attacks that evade traditional intrusion detection systems while exhausting server processing and memory. 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 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. - Test dispersion, maneuver, and adaptive response prototype systems with respect to program metrics. - Conduct exercises in collaboration with transition partners to obtain feedback on XD3 features, capabilities, and concepts of operation. ***FY 2019 Plans:*** - Incorporate feedback received during exercises, and re-test systems against program metrics to verify intended operation and desired transitionable features. - Test within service provider facilities by subjecting XD3 to DDoS attacks as observed in operational network environments. - Pursue transition to commercial network operators and DoD network service providers through demonstrations in their network environments. ***FY 2018 to FY 2019 Increase/Decrease Statement:***			

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency			**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
The FY 2019 decrease is the result of XD3 development work concluding and the focus shifting to demonstration in operational environments to establish utility for transition partners.			
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 cyber 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 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. - Assess the performance of components and the integrated CFAR system. ***FY 2019 Plans:*** - Demonstrate an integrated CFAR system that protects against a wide range of threats in an operational environment. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease is the result of development work concluding and the focus shifting to demonstration in an operational environment to establish utility for transition partners.	22.500	17.030	5.699
Title: Enhanced Attribution ***Description:*** The Enhanced Attribution program is developing technologies to associate the malicious actions of cyber adversaries to individual operators, and to publicly reveal these actions without compromising sources and methods. The program focuses on new approaches for identifying malicious cyber operators, analyzing their software tools and actions, and confirming this information with commercial and public sources of data. As the attribution techniques are developed and show promise, they will provide the basis for new cyber capabilities such as indications and warning of adversary cyber actions. These technologies will be implemented in tools for evaluation by potential transition partners. ***FY 2018 Plans:***	17.500	21.200	24.530

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency			**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
- Refine and expand the ontology for cyber actions to accommodate new adversary tactics, techniques, and procedures and to reduce the computational and bandwidth requirements of attribution modules. - Integrate attribution modules and demonstrate the capability to generate narrative descriptions of and indications and warning for adversary cyber operator actions. - Conduct evaluations against simulated threats in collaboration with transition partners. ***FY 2019 Plans:*** - Develop and demonstrate algorithmic support for distributed database deployment and query of operational cyber data. - Demonstrate automated narrative generation of adversary cyber operator activities. - Develop metrics that quantify risks to sensitive sources and methods in alternative attribution narratives. - Support transition partners in their evaluation of the attribution technologies. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase reflects continued development of the technologies and expanded evaluation of the software prototypes created to attribute adversary cyber operator actions and to automatically generate attribution narratives.			
Title: Active Social Engineering Defense (ASED) ***Description:*** The Active Social Engineering Defense (ASED) program, building on technology developed in the Enhanced Attribution program, will develop technologies to automatically identify, disrupt and investigate social engineering attacks via bot-mediated communications. Social engineering attacks, such as phishing and spear-phishing, typically gain user trust via impersonation to induce behaviors or elicit sensitive information that compromise security of an information system. At present, defending against social engineering attacks falls entirely to users. ASED aims to prevent social engineering attacks by creating counter-social-engineering bots that act on behalf of users to mediate and aggregate communications, and auto-identify attackers. If successful, ASED will greatly reduce the effectiveness of adversary social engineering attacks and improve the security of DoD information systems. ***FY 2018 Plans:*** - Develop the means to create synthetic social engineering attack data. - Design a standardized application programming interface to facilitate the integration of counter-social-engineering bot technologies. - Propose algorithms and big data approaches for bots to mediate and aggregate communications, and auto-identify attackers. - Initiate integration of a testbed for evaluating counter-social-engineering bots. ***FY 2019 Plans:*** - Use big data techniques to characterize internet communications and rapidly detect social engineering attacks. - Develop machine-learning-based intelligent bots that can actively engage with attackers.	-	16.000	25.000

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
- Develop initial capability for semi-automated attribution of social engineering attacks. - Assess performance of bot-based techniques to counter social engineering attacks using synthetic data. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of development work accelerating, technologies being integrated in an initial prototype system, and demonstrations on synthetic data.			
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 for DoD-scale information networks. 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 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 packet capture (PCAP), host system log, and netflow data, and construct feature sets for indicators of adversary activity. - Formulate mathematical approaches for managing network sensor data collection, transmission and retention policies to optimize cyber threat detection and characterization, and enhance enterprise-scale cyber situational awareness. - Initiate development of foundational protective measures. - Establish a test and evaluation environment to allow assessment of cyber threat detection and characterization techniques using real-world data. - Develop cyber security techniques for enterprise IT infrastructure. ***FY 2019 Plans:*** - Refine algorithms to process raw and summary cyber data, and construct feature sets for indicators of adversary activity such as credential misuse, data exfiltration, and lateral movement. - Demonstrate improved detection and identification capabilities using closed loop approaches for managing data collection, transmission, and retention. - Perform initial test and evaluation of the most promising cyber threat detection and protective measures through adversarial use cases drawn from real-world datasets including PCAP, host system log, and netflow data. - Demonstrate distributed algorithms to enhance enterprise-scale cyber situational awareness via tests using real-world data.	-	16.800	22.800

Exhibit R-2A, RDT&E Project Justification: PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
- Demonstrate cyber security techniques for enterprise IT infrastructure. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of development work accelerating, technologies being integrated in an initial prototype system, and demonstrations using real-world data.			
Title: Cyber Assured Systems Engineering (CASE) ***Description:*** The Cyber Assured Systems Engineering (CASE) program will develop the design, analysis and verification tools needed to allow system engineers to design-in cyber resiliency and manage tradeoffs as they do other nonfunctional properties when designing complex embedded computing systems. The current state of practice for cyber resilience utilizes penetration testing after system construction to drive post-design re-engineering. The CASE technical approach will be 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 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. ***FY 2018 Plans:*** - Develop baseline capability to derive resilience-related requirements before system design and construction. - Develop architectural design and analysis tools to verify derived resilience requirements while generating validation tests to run on the eventual implementation. - Develop software analysis tools to verify new resiliency properties in legacy software. - Formulate cyber resilience design challenge problems relevant to military cyber physical systems. ***FY 2019 Plans:*** - Create tools to adapt existing software to support system-level resilience requirements. - Develop techniques for translating the output of cyber resilience design tools into concepts relevant to the system designer. - Enhance inference engines, satisfiability solvers, and provers to scale to complex cyber physical systems. - Demonstrate and evaluate design tools and techniques on an initial cyber resilience design challenge problem. ***FY 2018 to FY 2019 Increase/Decrease Statement:***	-	17.000	21.400

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
The FY 2019 increase reflects continued development of techniques and software tools to enable systems engineers to design-in cyber resiliency requirements in a rigorous fashion and initial demonstrations on challenge problems.			
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) ***Description:*** The Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) program, building on technology developed in the Cyber Grand Challenge program, will develop safe and reliable autonomous software agents that can neutralize botnet implants and similar large-scale malware. HACCS will develop technologies to (1) identify and characterize botnet-conscripted networks of devices to determine the types of devices and the software services running on them with sufficient precision to infer the presence of known vulnerabilities; (2) generate software exploits for a large number of known vulnerabilities that can be used to establish initial presence in each botnet-conscripted network without disrupting system functionality; and (3) create high-assurance software agents that autonomously navigate within botnet-conscripted networks, identify botnet implants, and curtail their ability to operate, while minimizing side effects to systems and infrastructure. HACCS will enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations. ***FY 2018 Plans:*** - Initiate development of algorithms for identifying the command-and-control, attack, and activity traffic of botnet nodes. - Design architecture for automated generation of software exploits using high-level information about known vulnerabilities. - Explore formal approaches to verify correctness properties of autonomous software agents and use machine learning or similar artificial intelligence techniques to ensure safe and reliable autonomous agent behavior. ***FY 2019 Plans:*** - Enhance botnet-tracking algorithms by developing and incorporating techniques to detect stealthy and covert command-and-control protocols. - Scale vulnerability discovery and exploit generation techniques to complex software running on real operating systems. - Collaborate with transition partners to test counter-botnet autonomous agents on synthetic environments, and demonstrate the capability to characterize botnet-conscripted networks in terms of the number, types, and software versions of the compromised devices in those networks. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of development work accelerating, technologies being integrated in an initial prototype system, and demonstrations on synthetic environments.	-	10.727	21.000
Title: Symbiotic Cyber Operations* ***Description:*** *Formerly part of Automated Cyber Operations and Defense (ACOD)	-	4.000	13.500

Exhibit R-2A, RDT&E Project Justification: PB 2019 Defense Advanced Research Projects Agency		Date: February 2018
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 2017**	**FY 2018**	**FY 2019**
The Symbiotic Cyber Operations program will develop a semi-automated cyber operations system to enable operators to create and analyze cyber effects more rapidly and accurately than unaided human operators. The program envisions high-intensity cyber operations executed by computers under human supervision. To accomplish this, the program 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. This technology will automatically evaluate the defensive posture of software and networks during operations; triage and verify system security issues; determine adversary intent; and guide operator responses. Technologies to be developed and integrated may include binary analysis, case-based reasoning, abstract interpretation, reinforcement learning, game theory, and stochastic optimization. Through human-machine cyber teaming, Symbiotic Cyber Operations will ensure U.S. operational superiority in future cyber conflicts. ***FY 2018 Plans:*** - Initiate development of semantically rich human-computer interfaces for cyber reverse engineering and automated cyber capabilities to analyze defensive security postures. - Develop concepts of operations for mixed-initiative cyber operations. - Create semantic mappings from configuration settings to component functionality, and develop a representation of system functional requirements that enables automated reasoning to evaluate configuration security. ***FY 2019 Plans:*** - Develop a cyber operations reasoning framework to automatically identify which possible actions are allowable under rules of engagement, to rank alternative allowable actions in terms of likely efficacy, and to decide when a proposed action should proceed. - Implement interfaces that facilitate timely human understanding of rapid changes in cyberspace and effective human interaction with automated cyber defenses. - Implement automation modes and logic appropriate for use across the cyber conflict spectrum. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of development work accelerating and technologies being integrated in an initial prototype system.			
Title: Configuration Security* ***Description:*** *Formerly part of Automated Cyber Operations and Defense (ACOD) The Configuration Security program will develop technologies to analyze, monitor, and modify the configuration of composed cyber-physical-human systems to identify system vulnerabilities and minimize the attack surface while maintaining functionality and performance. Complex cyber-physical systems, such as ships, airplanes and critical infrastructure increasingly consist of	-	5.000	14.500

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
commodity information technology components. The manual configuration necessary to enable each component to interoperate introduces exploitable cyber vulnerabilities, as do the standard operating procedures that system operators follow. The Configuration Security program will develop capabilities to automate the appropriate configuration of such systems within the operational context. The resulting capability will ensure secure configuration settings and prevent malicious changes to these settings. ***FY 2018 Plans:*** - Formulate scalable approaches for generating secure configurations without exhaustive exploration of the configuration space. ***FY 2019 Plans:*** - Develop techniques to automatically generate secure configurations for composed cyber-physical-human systems including the capability to translate human standard operating procedures into machine-understandable formats. - Develop an initial capability to prevent malicious modification of configurations from the system-generated baseline. - Develop algorithms to reconfigure a system automatically to a safer, more secure baseline that assures required functionality. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase reflects expanded algorithm development.			
Title: Protecting C3 Networks (PC3N) ***Description:*** The Protecting C3 Networks (PC3N) program will develop technologies to make military command, control, and communications (C3) networks more resilient against adversary attempts to disrupt, deny, degrade, or destroy mission-critical information, hosts, network elements, or services. PC3N technologies will enable DoD network operators to fully leverage our inherent home field advantage when defending military networks and, ultimately, to neutralize adversary cyber tradecraft in real time. The program will also develop technologies to assure and, when required, restore network integrity in the aftermath of an attack. PC3N technology development will be coordinated with DoD network operators. ***FY 2019 Plans:*** - Develop an analytic framework for quantifying the resilience of a network to adversary attempts to disrupt, deny, degrade, or destroy mission-critical information, hosts, or network elements. - Identify network protocols requiring algorithmic improvements, and develop hardened protocol stacks to ensure delivery of critical services in spite of adversary cyber attacks on C3 networks. - Formulate trusted zeroization and related cryptographic approaches for recovery and assurance of C3 networks in the aftermath of an attack. ***FY 2018 to FY 2019 Increase/Decrease Statement:***	-	-	6.580

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
The FY 2019 increase reflects program initiation.			
Title: System Security Integrated Through Hardware and firmware (SSITH) ***Description:*** The System Security Integrated Through Hardware and firmware (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 2018 Plans:*** - 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 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease reflects the program moving to PE 0602716E, Project ELT-02.	11.000	18.500	-
Title: Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) ***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 are being developed in coordination with operational commands. ***FY 2018 Plans:*** - Demonstrate EdgeCT capabilities in overcoming impairments to command and control and related networked applications.	24.938	11.400	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
- Address and rectify operational vulnerabilities identified by red teams through additional design and testing activities within program testbeds. - Pursue transition to DoD's commercial network operators through demonstrations and testing within service provider facilities, subjecting EdgeCT to impairments observed in network environments. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease reflects program completion.			
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. ***FY 2018 Plans:*** - Demonstrate Plan X in transition partner systems. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease reflects program completion.	23.349	7.500	-
Title: Supply Chain Hardware Integrity for Electronics Defense (SHIELD) ***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 2018 Plans:*** - Continue functional and performance testing of manufactured SHIELD dielets. - Demonstrate the SHIELD concept of operation in an actual or environmental facsimile of an integrated circuit supply chain.	16.000	5.000	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
- Incorporate SHIELD dielets into integrated circuit (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. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease reflects program completion.			
Title: Vetting Commodity Computing Systems for the DoD (VET) ***Description:*** The Vetting Commodity Computing Systems for the DoD (VET) program developed 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 detect hidden malicious functionality and also the software and firmware defects and vulnerabilities that can facilitate adversary cyber attack.	12.350	-	-
Title: High Assurance Cyber Military Systems (HACMS) ***Description:*** The High Assurance Cyber Military Systems (HACMS) program developed and demonstrated 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 are within reach at reasonable costs. The program developed, matured, and integrated these technologies to produce an embedded computing platform that provides a high level of assurance for mission-critical military applications. Additionally, the program explored 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.	10.300	-	-
Title: Cyber Grand Challenge (CGC) ***Description:*** The Cyber Grand Challenge (CGC) program created automated defenses that identified and responded to cyber attacks more rapidly than human operators. CGC technology monitored defended software and networks during operations, reasoned about flawed software, formulated effective defenses, and deployed defenses automatically. Technologies developed and integrated included anomaly detection, Monte Carlo input generation, case-based reasoning, heuristics, game theory,	6.905	-	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
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 incentivized competition through a Grand Challenge in which CGC technologies competed head-to-head.			
Accomplishments/Planned Programs Subtotals	243.642	260.757	259.359

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

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

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency			**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
IT-04: *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*	-	55.858	82.108	80.073	-	80.073	90.842	81.936	89.921	89.921	-	-

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 perform critical missions safely and with high degrees of autonomy. The technologies developed in this project will lay the foundation for a new generation of human-machine systems for the U.S. military.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Title: Explainable Artificial Intelligence (XAI)	11.090	18.446	22.000

Description: 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 2018 Plans:
- Develop and demonstrate an initial prototype using modified deep learning techniques to produce deep neural nets that are more interpretable than current techniques.
- Develop and demonstrate an initial prototype using structured, causal, machine learning techniques that are inherently more interpretable.

B. Accomplishments/Planned Programs ($ in Millions)

- Develop and demonstrate an initial prototype that creates an explainable model for an existing black box machine learning system.

FY 2019 Plans:

- Formulate second-generation explainable machine learning methods and modified deep learning techniques, and integrate these into prototypes.
- Define a set of common test problems in data analytics and autonomous systems for evaluating explanation effectiveness.
- Deliver a computational model of the theory of explanation in artificial intelligence, and demonstrate the ability of the computational model to predict the performance of explanations generated by the systems.

FY 2018 to FY 2019 Increase/Decrease Statement:

The FY 2019 increase reflects continued development of explainable machine learning techniques and integration for testing on problems in data analytics and autonomous systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Title: Active Interpretation of Disparate Alternatives (AIDA)	5.500	17.300	21.100

Description: The Active Interpretation of Disparate Alternatives (AIDA) program is developing a multi-hypothesis semantic engine that generates alternative interpretations of events, situations, and trends from a variety of unstructured sources for use in environments where there are noisy, conflicting, and potentially deceptive data. At present, 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. AIDA seeks to develop and demonstrate technology to automatically map information derived from multiple sources into a common semantic representation, aggregate information, resolve ambiguities, discover conflicting information, and generate and explore multiple interpretations of events, situations, and trends. If successful, AIDA will provide decision makers a capability to understand alternative explanations for available information and to make contingency plans accordingly.

FY 2018 Plans:

- Define an initial common semantic representation language for diverse sources.
- Adapt multimedia-analysis algorithms to produce information suitable for use in a common semantic representation.
- Develop semantic techniques that automatically generate, update, rank, and prune alternative interpretations given new data.
- Develop techniques to assess the possibility that an interpretation is based on semantically consistent adversarial misinformation.

FY 2019 Plans:

- Develop techniques to integrate diverse information from multiple sources into the common semantic representation.
- Develop techniques to extend known ontologies using information from diverse sources.
- Develop techniques to estimate the confidence of the generated interpretations.

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**

- Evaluate techniques to identify semantically consistent adversarial misinformation on synthetic data.

FY 2018 to FY 2019 Increase/Decrease Statement:
The FY 2019 increase reflects continued development of techniques for generating multiple alternative interpretations from multimedia data and conducting adversarial evaluations of techniques on synthetic data.

Title: Low Resource Languages for Emergent Incidents (LORELEI)	25.636	28.662	13.880

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 2018 Plans:
- Extend development of techniques to determine strength of opinions and beliefs in low-resource language speech as well as text.
- Integrate multiple new algorithms with a graphical user interface, and evaluate with end users.
- Construct an integrated system employing multiple algorithms for low-resource language analysis.
- Evaluate performance on the Uyghur language baseline and on additional low-resource languages.

FY 2019 Plans:
- Develop techniques to establish situational awareness from text and speech of low-resource languages.
- Extend development of techniques to determine strength of opinions and beliefs to understand urgency and completion status of emerging situations.
- Evaluate performance on additional languages, and measure progress on the languages evaluated in the previous year.

FY 2018 to FY 2019 Increase/Decrease Statement:
The FY 2019 decrease is the result of development work concluding and the focus shifting to testing on a diverse collection of low-resource languages.

Title: Assured Autonomy	-	14.700	18.020

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
Description: The Assured Autonomy program, an outgrowth from the Explainable Artificial Intelligence program, will develop rigorous design and analysis technologies for continual assurance of learning-enabled autonomous systems to guarantee safety properties in uncertain environments. Currently, the state of art for test, evaluation, verification and validation is only applicable to non-learning systems operating in well-characterized environments. As a result, autonomous systems enabled by machine learning (e.g., deep neural nets for perception, reinforcement learning for control policies, and online model learning) lack rigorous safety assurance. Assured Autonomy is developing new techniques for modeling and system design, formal verification, simulation-based testing, machine learning, and safety-assured learning to provide continual assurance of learning-enabled autonomous systems. The technologies being developed in Assured Autonomy will enable the DoD to more rapidly and efficiently deploy learning-enabled autonomous systems that can be trusted to operate safely in uncertain environments. ***FY 2018 Plans:*** - Develop initial algorithms for formal representation and online evaluation of assurance cases, safety-aware learning, and enforcement of safety constraints. - Develop and design verification tools that predict properties and prove correctness of systems with learning-enabled components. - Produce assurance challenge problems for different learning-enabled autonomous systems. ***FY 2019 Plans:*** - Develop techniques and tools that construct formal semantics of assurance cases, provide dynamic interpretation of assurance cases, and modularize and automatically generate assurance cases from system design descriptions. - Develop algorithms that integrate and enforce safety constraints in learning-enabled algorithms. - Apply technologies to several learning-enabled autonomous platforms, and assess their reliability and sensitivity to modeling assumptions. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase is the result of the development work accelerating and technologies being tested on several learning-enabled autonomous platforms.			
Title: Human-Machine Symbiosis (HMS) ***Description:*** The Human-Machine Symbiosis (HMS) program will develop technologies to enable machines to collaborate with humans as colleagues, partners, and teammates. The world is moving faster than humans can assimilate, understand, and act. At present, we design machines to handle well-defined, high-volume or high-speed tasks, freeing humans to focus on complexity. If successful, HMS technologies will enable machines to do more than execute pre-programmed instructions. Rather, HMS-enabled machines will understand speech; extract information contained in diverse media; learn, reason and apply knowledge gained through experience; identify and work to fill knowledge gaps; extrapolate causal phenomena to anticipate predictable	-	-	5.073

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
developments; respond intelligently to new and unforeseen events; and exhibit behaviors that are typically believed to require common sense. HMS application areas include cyberspace operations and command and control. ***FY 2019 Plans:*** - Explore meta-knowledge architectures that capture imprecision, uncertainty and errors, identify knowledge gaps, and enable machines to reason about their state of knowledge. - Formulate perceptually-grounded representations to enable commonsense reasoning by machines about the physical world and spatio-temporal phenomena. - Develop quantitative approaches for creating high-performing human-machine teams of individuals and semi-autonomous systems with complementary characteristics/capabilities. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase reflects program initiation.			
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 technologies will extract knowledge at scale for open source intelligence and threat analysis. Transition partners include the intelligence community and operational commands. ***FY 2018 Plans:*** - Design and implement an open evaluation with thousands of documents in multiple languages as input, and a single aggregate language-independent knowledge base that includes entities, events, relations, and sentiment as output. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 decrease reflects program completion.	13.632	3.000	-
Accomplishments/Planned Programs Subtotals	55.858	82.108	80.073

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Defense Advanced Research Projects Agency		**Date:** February 2018
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 **/** *LANGUAGE UNDERSTANDING AND SYMBIOTIC AUTOMATION*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

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