Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Defense Advanced Research Projects Agency	Date: March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	379.578	404.967	442.556	-	442.556	435.746	461.923	494.810	506.254	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	48.006	52.184	22.538	-	22.538	39.630	55.730	65.730	65.730	-	-
IT-03: *CYBER SECURITY*	-	262.375	255.919	258.850	-	258.850	229.254	235.940	247.159	251.603	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	69.197	96.864	161.168	-	161.168	166.862	170.253	181.921	188.921	-	-

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 Cyber Security project is developing the computing, networking, and cyber security technologies required to protect DoD, U.S. government, and U.S. civilian information, information infrastructure, and mission-critical information systems. Information technologies enable important new military capabilities and drive the productivity gains essential to U.S. industry.

The Artificial Intelligence and Human-Machine Symbiosis project develops technologies to enable machines to function not only as tools that facilitate human action but as trusted partners to human operators. Of particular interest are systems that can understand human speech and extract information contained in diverse media; answer questions, reach conclusions, and propose explanations; and learn, reason and apply knowledge gained through experience to respond intelligently to new and unforeseen events. Enabling computing systems with such human-like intelligence is now of critical importance because the tempo of military operations in emerging domains exceeds that at which unaided humans can orient, understand, and act.

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Defense Advanced Research Projects Agency	Date: March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	392.784	395.317	376.946	-	376.946
Current President's Budget	379.578	404.967	442.556	-	442.556
Total Adjustments	-13.206	9.650	65.610	-	65.610
• Congressional General Reductions	0.000	-15.350			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	25.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	0.000	0.000			
• SBIR/STTR Transfer	-13.206	0.000			
• TotalOtherAdjustments	-	-	65.610	-	65.610

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2018	FY 2019
Project: IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*		
Congressional Add: *DARPA Foundational and Applied Artificial Intelligence*	-	25.000
Congressional Add Subtotals for Project: IT-04	-	25.000
Congressional Add Totals for all Projects	-	25.000

Change Summary Explanation

FY 2018: Decrease reflects SBIR/STTR transfer.

FY 2019: Increase reflects Congressional adjustments.

FY 2020: Increase reflects new start artificial intelligence programs in the Artificial Intelligence and Human-Machine Symbiosis project.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency			Date: March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	48.006	52.184	22.538	-	22.538	39.630	55.730	65.730	65.730	-	-

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 2018	FY 2019	FY 2020
Title: Spectrum Collaboration Challenge (SC2)	18.000	25.184	2.000
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 2019 Plans:*** - Hold a second competition, to take place on the custom-built competition testbed. - Identify transition partner for the testbed post competition final event.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
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 2018	FY 2019	FY 2020
- Develop final competition event execution plan. ***FY 2020 Plans:*** - Execute a live championship event with an international audience of 1,000+ at Mobile World Congress Americas. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease in FY 2020 reflects program completion.			
Title: RF Machine Learning Systems (RFMLS) ***Description:*** The RF Machine Learning Systems (RFMLS) program is addressing the performance limitations of conventional radio frequency (RF) systems such as radar, signals intelligence, electronic warfare, and communications. The performance of future RF systems in the DoD will be defined by their ability to adapt and respond to their environment in real-time. We currently lack both the algorithms and computational power to manage the volume of data and complexity of decision-making that will be required. RFMLS technology will develop machine learning techniques that are able to help manage this complexity by, for example, recognizing specific emitters or detecting anomalies in a cluttered environment. The objective of the RFMLS program is to both develop these foundational technologies and to apply them to relevant DoD systems. ***FY 2019 Plans:*** - Evaluate integratability of machine learning algorithms and architectures with candidate DoD RF hardware systems. - Complete first phase development of machine learning algorithms and architectures for the four challenge problems. - Test preliminary performance of solutions for the four challenge problems. - Complete development of an RF hardware system to host field testing and demonstrations. ***FY 2020 Plans:*** - Complete final phase development of machine learning algorithms and architectures for the four challenge problems. - Create test and demonstration plan for final open-air demonstration of RFMLS algorithms. - Begin integration of machine learning solutions into an RF hardware system to host field testing and demonstrations. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The decrease in FY 2020 reflects completing the process of demonstrating machine learning algorithms on a test platform.	10.000	27.000	20.538
Title: Hierarchical Identify Verify Exploit (HIVE) ***Description:*** The Hierarchical Identify Verify Exploit (HIVE) program is pursuing new hardware architectures and algorithms for improving the efficiency of graph and sparse data analytics. When developing operationally significant intelligence, human analysts today are forced to reduce the scope of the problems that they can address and the tempo of their analyses due to the limitations of currently deployed hardware. Because of these limitations the amount of information gathered is quickly outstripping	18.006	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
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 2018	FY 2019	FY 2020
the human ability to review, process, fuse, and interpret. To resolve this challenge, HIVE seeks to leverage improvements in computational efficiency 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 battlespace in real time. The HIVE program moves to PE 0602716E/ Project ELT-02 in FY 2019.			
Title: Electronic Globalization ***Description:*** The Electronic Globalization effort aimed 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 pursued 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 supported the development of key risk-reduction techniques including advanced imaging and computational methods for identifying an IC's functional elements.	2.000	-	-
Accomplishments/Planned Programs Subtotals	48.006	52.184	22.538

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 2020 Defense Advanced Research Projects Agency			Date: March 2019
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-03 / *CYBER SECURITY*	

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	262.375	255.919	258.850	-	258.850	229.254	235.940	247.159	251.603	-	-

A. Mission Description and Budget Item Justification

The Cyber Security project is developing the computing, networking, and cyber security technologies required to protect DoD, U.S. government, and U.S. civilian information, information infrastructure, and mission-critical information systems. Information technologies enable important new military capabilities and drive the productivity gains essential to U.S. industry. Meanwhile, cyber threats grow in sophistication and number, and put sensitive data, classified computer programs, mission-critical information systems, and U.S. economic competitiveness at risk. The technologies developed in this project will enhance the resilience of information systems to current and emerging cyber threats; enable broad situational awareness of the cyber domain; and provide the basis for accurate, calibrated, and safe cyber response.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Cyber-Hunting at Scale (CHASE)	16.344	21.800	23.600
Description: The Cyber-Hunting at Scale (CHASE) program is developing 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 a great many devices. CHASE is developing novel algorithms and analysis tools to dynamically collect data from across the network, actively hunt for advanced threats that evade routine security measures, and automatically disseminate protective measures that bolster the collective cyber defense posture. ***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 raw packet capture (PCAP), host system log, and netflow data. - Demonstrate distributed algorithms to enhance enterprise-scale cyber situational awareness via tests using real-world data. ***FY 2020 Plans:*** - Integrate threat detection, threat characterization, and data planning components, and demonstrate integrated data management feedback loops in real networks. - Evaluate effectiveness of threat detection and data planning components using operational datasets from transition partners. - Integrate foundational protective measures for adversarial actions such as data exfiltration and lateral movement.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Demonstrate global analysis methods and foundational protective measures on distributed enterprise networks. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase is the result of development work continuing, integration work increasing, and expanded demonstration and evaluation efforts on distributed enterprise networks.			
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) ***Description:*** The Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) program is developing safe and reliable autonomous software agents that can neutralize botnet implants and similar large-scale malware. HACCS is developing 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 technologies will enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations. ***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 in synthetic environments, and demonstrate the capability to characterize botnet-conscripted networks. ***FY 2020 Plans:*** - Expand vulnerability discovery techniques for additional classes of software bugs. - Evaluate botnet-tracking algorithms for detecting stealthy and covert command-and-control protocols. - Evaluate autonomous agent behavior in contained environments. - Collaborate with transition partners to determine how counter-botnet technologies may be integrated into existing architectures. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase is the result of continued counter-botnet technology development and prototype integration work, and expanded demonstrations on synthetic environments in collaboration with transition partners.	15.248	19.000	22.500
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	35.386	27.310	22.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020

Description: The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is developing automated systems to enable a black start recovery of the U.S. power grid amidst a cyber attack on the energy sector's critical infrastructure. This approach will enable skilled cyber and power engineers to rapidly restore electrical service after an attack that challenges the recovery capabilities of the impacted organizations (e.g., utilities, balancing authorities, independent system operators, bulk power markets). 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 2019 Plans:
- Develop robust capability for grid physics anomaly and Supervisory Control and Data Acquisition (SCADA) spoofing detection.
- 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, isolation, and characterization of cyber weapons targeting a wide range of industrial control system (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 operationally-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 2020 Plans:
- Refine capabilities to detect, correlate, and report grid physics anomalies at scale across multiple disparate utilities.
- Develop communications prototype optimizing the use of available communication channels in a contested environment to coordinate cyber first responder and utility actions.
- Develop prototypes to quickly perform cyber forensic analysis and restore operational functionality of ICS/SCADA equipment for continued operations.
- Prototype capabilities to maintain and expand situational awareness and a trusted operational picture.
- Conduct capstone exercise demonstrating operational impact of prototypes, and prepare tools for technology transition.

FY 2019 to FY 2020 Increase/Decrease Statement:

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
The FY 2020 decrease reflects ramping down of development and integration of prototypes for rapid recovery of the power grid from a cyber attack, continuation of exercises to establish technology operational readiness, and technology transition.			
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 2019 Plans:*** - Develop and demonstrate scalable algorithms for querying cyber data across multiple databases. - Demonstrate automated narrative generation of adversary cyber operator activities. - Develop metrics that quantify risks to sources and methods in alternative attribution narratives. - Collaborate with transition partners to evaluate attribution technologies in operationally relevant scenarios. ***FY 2020 Plans:*** - Integrate event extraction techniques into an attribution fusion platform. - Develop and evaluate predictive analytic algorithms for anticipating adversary actions across a cyber campaign. - Develop and evaluate adversary pattern matching algorithms for discovering previously unknown campaigns. - Support transition partners in their evaluation of the attribution and narrative generation technologies in realistic scenarios. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects minor program repricing.	21.214	20.830	21.500
Title: Dispersed Computing ***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 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-	17.000	18.000	20.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
purposed network-compute elements make it possible to eliminate bottlenecks/chokepoints and to 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 2019 Plans:*** - Implement integrated prototype network-compute elements that incorporate dispersed computation algorithms and programmable protocol stack functionality. - Develop a user interface that enables operators to understand how the dispersed network computation elements are performing as a unified system on applications of interest. - Stand up a large-scale testbed to simulate real-world environments, test integrated prototypes at scale, and conduct demonstrations of prototypes. ***FY 2020 Plans:*** - Develop automated mechanisms for redistributing workloads across dispersed network computation elements to achieve reliable and near-optimal performance even in the presence of dynamic failures and impairments. - Extend the user interface to provide operators with fine-grained visibility into the workloads being handled by the dispersed network computation elements on applications of interest. - Evaluate integrated prototype network-compute elements and demonstrate prototypes to Defense Information Systems Agency and commercial network providers. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects continued development of the technologies and software prototypes for distributing workloads to network-compute elements, and expanded testing and demonstration for potential transition partners.			
Title: Computers and Humans Exploring Software Security (CHESS)*	7.500	13.000	18.900
Description: *Formerly Symbiotic Cyber Operations The Computers and Humans Exploring Software Security (CHESS) program is developing technologies to enable computers and humans to reason collaboratively over software artifacts, such as source code and compiled binaries, with the goal of finding vulnerabilities more rapidly and accurately than unaided human operators. CHESS envisions a future in which high-intensity cyber operations are conducted by computer-human teams. CHESS capabilities will be designed for use by humans of varying skill levels, even those with no previous cyber experience or relevant domain knowledge. Achieving the necessary scale and timelines in vulnerability discovery will require innovative combinations of automated program analysis techniques with support for			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
advanced computer-human collaboration. Combining human-generated insight into the vulnerability discovery process with the speed and scale of computational analysis will be a critical enabler for U.S. operational cyber superiority. ***FY 2019 Plans:*** - Develop instrumentation to capture and analyze the process by which humans reason over software to provide a basis for developing new forms of highly effective communication and information sharing between computers and humans. - Create contextually sensitive cyber reasoning techniques to address vulnerability classes that currently require human insight. - Generate representations of information gaps revealed by cyber reasoning systems to facilitate resolution by humans of varying skill levels. ***FY 2020 Plans:*** - Develop techniques for emitting a proof of vulnerability to confirm existence of a vulnerability, and for generating a non-disruptive, specific patch to neutralize the vulnerability. - Implement emerging vulnerability discovery techniques in an initial proof-of-concept computer-human software reasoning system. - Assess computer-human vulnerability discovery techniques on a synthetic vulnerability challenge corpus representative of complex software packages. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase is the result of development work accelerating, additional work to integrate technologies in a proof-of-concept computer-human software reasoning system, and initial performance assessments on a synthetic challenge corpus.			
Title: Configuration Security	6.930	16.230	18.000
Description: The Configuration Security program is developing 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 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 2019 Plans:*** - Develop techniques to automatically generate baseline secure configurations for simple composed cyber-physical-human systems for which informal systems engineering descriptions are available.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Design algorithms to reconfigure a system automatically to a safer, more secure baseline that assures the functionality specified in informal systems engineering descriptions. - Develop an initial capability to detect the malicious modification of configurations from the system-generated baseline for a single operational context. ***FY 2020 Plans:*** - Develop techniques to automatically generate baseline secure configurations for complex composed cyber-physical-human systems, including the translation of human-readable standard operating procedures into machine-understandable formats. - Develop algorithms to reconfigure a system automatically to a safer, quantifiably more secure baseline that assures required functionality and can justify the new configuration parameter selection with generated human-readable explanations. - Mature a capability to both detect and prevent malicious modification of configurations from the system-generated baseline, and to assist system operators in changing between operational contexts. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded algorithm and software development, and initial demonstration of an automated capability to detect and prevent malicious modification of configurations from the system-generated baseline.			
Title: Cyber Assured Systems Engineering (CASE)	24.937	21.400	17.000
Description: The Cyber Assured Systems Engineering (CASE) program is developing 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 formulates 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 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Formulate approaches for representing the intent of software and its abstract constraints separately from its concrete instantiation to enable rapid code synthesis and continual adaptation. - Demonstrate and evaluate design tools and techniques on an initial cyber resilience design challenge problem. ***FY 2020 Plans:*** - Enhance cyber resilience design tools based on the results of initial cyber resilience challenge problem. - Demonstrate and evaluate design tools and techniques on exemplar cyber-physical systems. - Integrate cyber resilience design tools into the engineering workflow of a defense system provider. - Use integrated design tools to re-engineer a portion of a defense platform to improve cyber resiliency. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease reflects ramping down development of techniques and software tools to enable systems engineers to design-in cyber resiliency requirements in a rigorous fashion, and expanded demonstrations on exemplar cyber-physical challenge problems.			
Title: Active Social Engineering Defense (ASED) ***Description:*** The Active Social Engineering Defense (ASED) program is developing 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 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. - Develop initial capability for semi-automated attribution of social engineering attacks. - Assess performance of bot-based counter-social-engineering techniques on synthetic attack data. ***FY 2020 Plans:*** - Create capability to autonomously detect social engineering attacks across multiple communication platforms. - Demonstrate semi-automated attribution of social engineering attacks. - Develop initial capability for multiple, coordinated counter-social-engineering bots to conduct fully-autonomous investigations of social engineering attacks.	10.000	15.524	13.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Perform evaluations to determine effectiveness and efficiency of social engineering detection and investigation techniques. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease is the result of development work ramping down as program focus shifts to evaluating the performance of the social engineering detection and investigation technologies.			
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 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 Internet of Things (IoT) devices and more complex devices such as thin-clients, feature phones, smart phones, laptops, and servers. - Characterize and model the signals from complex 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 2020 Plans:*** - Explore distance/accuracy tradeoffs for discriminating between known/unknown code running on a device, and develop techniques to improve performance by integrating multiple analog side channels. - Extend and apply signal analysis techniques to highly complex devices, including those with field programmable gate arrays. - Support potential transition partners in test and evaluation. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease is the result of development work ramping down and the focus shifting to optimization of techniques for use in operational environments and technology transition.	16.700	15.300	12.000
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.	17.000	18.870	6.520

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
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 2019 Plans:*** - Scale up secure multiparty computation, secure database queries, differential privacy, and remote attestation techniques to U.S. government and DoD data repositories. - Demonstrate privacy-preserving communication and collaboration techniques in real-world exercises on enterprise networks. - Incorporate privacy-preserving technologies in flexible toolkits and transition to U.S. government and DoD partners. ***FY 2020 Plans:*** - Extend techniques to address challenging use cases such as collaborative surveillance allocation and privacy-preserving combination of sensitive data sets. - Participate in exercises that demonstrate privacy protection in data communication and collaboration with allies and non-governmental organizations. - Transition secure multi-party computation libraries and privacy preserving technologies to open source repositories and to U.S. government and DoD partners. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease is the result of development work ramping down, continued efforts to demonstrate technologies on U.S. government and DoD use cases, and technology transition.			
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 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 2019 Plans:*** - Incorporate feedback received during exercises to enhance maneuver, deception, dispersion, and on-host adaptation techniques.	20.386	12.500	5.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Test and verify the intended operation of the prototype defensive architectures by subjecting techniques to simulated DDoS attacks. - Pursue transition to DoD network service providers and commercial network operators through demonstrations in operational network environments. ***FY 2020 Plans:*** - Harden technologies and complete transition to DoD network service providers and commercial network operators. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease is the result of XD3 development work concluding and the focus shifting to hardening technologies for transition partners.			
Title: Memory Optimization (MemOp) ***Description:*** The Memory Optimization (MemOp) program, building upon technologies developed in the Dispersed Computing program, will develop technology to optimize memory transactions in large scale computing systems. The demand for computing services is growing within both the U.S. government and commercial industry. In response, new technical approaches are being developed to provide massive computation efficiently and cost effectively. In particular, distributed data centers with high-speed interconnects and customizable hardware including graphics processing units (GPU) and field programmable gate arrays (FPGAs) are being used by service providers to achieve greater efficiency and improved processing performance. MemOp will explore new memory architectures that more fully leverage emerging customizable hardware to deliver computing services reliably and at reduced cost. The more promising MemOp memory architectures will be implemented and evaluated in hardware and software. The technologies developed in MemOp will provide enhanced efficiency and improved performance for large scale computing systems. ***FY 2019 Plans:*** - Formulate approaches, algorithms, and architectures for optimizing memory transactions in large scale computing systems. - Identify commercial off-the-shelf (COTS) and governments off-the-shelf (GOTS) hardware and software systems appropriate for modifications and testing of techniques for optimizing memory transactions. ***FY 2020 Plans:*** - Reduce the complexity of algorithms that map software tasks to processing units to achieve scalability to large scale memory systems. - Develop methods to interface to memory and develop accelerated processing pipelines for optimizations of interest. - Establish a test-bed to evaluate memory transaction improvements in systems incorporating GPUs and FPGAs.	-	8.955	22.200

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Implement algorithms and architectures for improving memory transaction performance in hardware and software and evaluate on MemOp test-bed. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded efforts to develop memory interface methods, accelerated processing pipelines, and an evaluation test-bed.			
Title: Resilient Anonymous Communication for Everyone (RACE) ***Description:*** The Resilient Anonymous Communication for Everyone (RACE) program, building on technologies pioneered within the SafeWare program (PE 0601101E, Project CYS-01), will develop cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient, mobile communications within a network environment. RACE will develop a mobile phone application and distributed systems that provide a secure message-passing service by combining advances in distributed system tasking with communication protocol encapsulation methods. The RACE system will maintain confidentiality, integrity, and availability of messaging while preventing large-scale compromise of the system. RACE security will be based on rigorous security arguments or in statistical arguments based on realistic simulations, and not on ad hoc security claims. ***FY 2019 Plans:*** - Formulate concepts for combining distributed system tasking, secure multiparty computation, and communication protocol encapsulation technologies in a message-passing system that cannot be compromised by a cyber adversary in a network environment. ***FY 2020 Plans:*** - Develop and implement techniques to prevent a cyber adversary from discovering the presence of and compromising the secure message-passing system by obfuscating communication protocols and encrypting data on the nodes at all times, even during computation. - Build an initial secure message-passing system that can defeat the efforts of a cyber adversary with limited ability to observe the network. - Initiate development of a test-bed on which to evaluate implementations of the obfuscation and cryptographic technologies and the integrated secure message-passing system against a simulated cyber adversary. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded development of obfuscation and encryption technologies, initial implementation of a secure message-passing system, and construction of a test-bed on which to evaluate the system against a simulated cyber adversary.	-	7.000	17.300
Title: Cora	-	7.400	12.430

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Description: The Cora program, building on technologies pioneered in the Memex program (PE 0602702E, Project TT-13), will develop technologies to enable machines to read heterogeneous text-based data sources, extract key entities and activities, and characterize cyber threats. Large volumes of text-based data contain scattered clues about the activities of cyber threats. Automated machine reading and analysis capabilities are required due to the extreme rates at which this text-based data is generated. In addition, the connections between extracted entities and their activities can be very subtle and, because they are buried in noise, difficult to detect and correlate. The Cora technologies will benefit cyber analysts by providing them with pre-processed cyber leads that might otherwise not be available. ***FY 2019 Plans:*** - Develop machine reading and entity extraction approaches for cyber analysis of text-based data. - Formulate techniques for correlating the activities of extracted cyber entities across large text corpora. - Initiate development of a large-scale platform for evaluating cyber analytical technologies. ***FY 2020 Plans:*** - Implement machine reading, cyber entity extraction, and activity correlation techniques in an integrated software system. - Evaluate cyber analytical technologies on large-scale data and implement algorithmic improvements to address scalability and performance. - Provide initial software capabilities to potential transition partners for performance assessments in operational environments. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded efforts to develop an integrated cyber analytical system, expanded evaluation on large-scale data, and technology transition.			
Title: Searchlight* ***Description:*** *Formerly Protecting C3 Networks (PC3N) The Searchlight program will develop technologies to ensure quality-of-service (QoS) guarantees are met for distributed applications operating across the Internet. The increasing use of Internet-based distributed applications creates risks as surges in network use can result in resource shortfalls. Searchlight will develop novel approaches for allocating inherently limited network resources to optimize the performance of distributed applications. Searchlight techniques and systems will enable organizations to adapt the QoS for their low-priority traffic to result in improved QoS for their high-priority traffic without affecting traffic from other Internet users. ***FY 2019 Plans:***	-	3.800	6.900

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Formulate big data and machine learning based schemes for adapting the QoS of low-priority distributed applications to improve the QoS of high-priority distributed applications. ***FY 2020 Plans:*** - Define a unified framework for network QoS requirements for diverse distributed applications. - Define metrics for the integrated QoS of a heterogeneous suite of distributed applications having differing and dynamic priorities. - Implement QoS adaptation schemes on programmable network elements such as software-defined routers and switches. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded development work to implement QoS adaptation schemes on programmable network elements.			
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 are being developed in coordination with operational users. ***FY 2019 Plans:*** - Demonstrate an integrated CFAR system that protects against a wide range of threats in an operational environment. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease reflects program completion.	17.030	6.000	-
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. EdgeCT algorithms and software prototypes are implemented 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 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 enables highly reliable networked communication for the military in the face of a wide variety of common network failure modes as well as cyber attacks	9.280	3.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
against network infrastructure. EdgeCT technologies are developed in coordination with operational commands and commercial service providers. ***FY 2019 Plans:*** - Harden technologies and complete transition to DoD's commercial network operators. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease reflects program completion.			
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. The SSITH program moves to Project ELT-02, Beyond Scaling Technology, in FY 2019.	18.420	-	-
Title: Supply Chain Hardware Integrity for Electronics Defense (SHIELD) ***Description:*** The Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program aimed 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 sought to incorporate a small, inexpensive silicon chip ("dielet") into the packaging of genuine components. The dielet provided 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 fulfilled a large, pressing, and evolving need for anti-counterfeit technologies.	5.000	-	-
Title: Plan X	4.000	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Description: The Plan X program developed technologies 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 created new graphical interfaces that enable intuitive visualization of events on hosts and networks to aid in the planning and execution of cyber warfare, and operationally meaningful measures to assess the effectiveness of cyber warfare missions.			
Accomplishments/Planned Programs Subtotals	262.375	255.919	258.850

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 2020 Defense Advanced Research Projects Agency			Date: March 2019
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	Project (Number/Name) IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	69.197	96.864	161.168	-	161.168	166.862	170.253	181.921	188.921	-	-

A. Mission Description and Budget Item Justification

The Artificial Intelligence and Human-Machine Symbiosis project develops technologies to enable machines to function not only as tools that facilitate human action but as trusted partners to human operators. Of particular interest are systems that can understand human speech and extract information contained in diverse media; answer questions, reach conclusions, and propose explanations; and learn, reason, and apply knowledge gained through experience to respond intelligently to new and unforeseen events. Enabling computing systems with such human-like intelligence is now of critical importance because the tempo of military operations in emerging domains exceeds that at which unaided humans can orient, understand, and act. The technologies developed in the Artificial Intelligence and Human-Machine Symbiosis project 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 and semi-autonomous agents to perform critical missions in contested physical and virtual environments safely and reliably.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Explainable Artificial Intelligence (XAI)	17.446	18.830	26.050
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, data analytics, and decision-support systems. ***FY 2019 Plans:*** - Evaluate the performance of the initial prototype systems against developer-selected test problems in autonomy and data analytics. - Formulate improved explainable machine learning methods and modified deep learning techniques, integrate these into prototypes, and refine and test.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Define a set of test problems in data analytics and autonomous systems for understanding explanation effectiveness of the systems. - Refine 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 2020 Plans:*** - Evaluate the performance and the explanation effectiveness against government-selected test problems in autonomy and data analytics. - Optimize explainable machine learning techniques and user interfaces for integration into prototype systems. - Expand the set of test problems in data analytics and autonomous systems for evaluating explanation effectiveness of the systems. - Refine the computational model of explanation, and show increased ability to predict the performance of explanations generated by the systems. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects continued development of explainable machine learning techniques, accelerated integration of techniques in machine learning systems, and expanded testing on problems in data analytics and autonomous systems.			
Title: Assured Autonomy	15.700	17.520	25.550
Description: The Assured Autonomy program is developing rigorous design and analysis technologies for continual assurance of learning-enabled autonomous systems to guarantee safety properties in uncertain environments. Currently, the state of the 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 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 systems.			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Produce assurance challenge problems for different learning-enabled autonomous systems, and evaluate the effectiveness of safety-aware learning and safety constraint enforcement techniques. ***FY 2020 Plans:*** - Develop scalable methods addressing formal verification of safety properties of learning-enabled autonomous systems and scalable algorithms for dynamic evaluation of assurance cases. - Construct monitors to detect data-distribution shifts as the operating environment diverges from the training environment. - Assess the reliability and sensitivity of techniques to modeling assumptions for different learning-enabled autonomous systems. - Apply technologies to assurance challenge problems for several learning-enabled autonomous platforms of interest to the DoD. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase is the result of development work accelerating and technologies being tested on several learning-enabled autonomous platforms.			
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 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 2019 Plans:*** - Develop scalable automated techniques to integrate diverse information from multiple high-volume sources into the common semantic representation. - Develop techniques to extend and evolve existing ontologies using information from diverse sources. - Develop techniques to estimate the confidence of the generated interpretations, and formulate approaches for evaluating the accuracy of confidence estimates. - Evaluate techniques to identify semantically consistent adversarial misinformation on synthetic data. ***FY 2020 Plans:*** - Enhance multimedia analytics through use of feedback from generated hypotheses. - Develop techniques to limit the over-generation of hypotheses by automatically discarding irrelevant or duplicated hypotheses.	16.850	17.780	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
- Develop an intuitive interface to allow users to modify the extracted semantic elements and the generated hypotheses at any stage of the analysis. - Collaborate with transition partners to assess the validity and completeness of generated hypotheses using real-world data. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects continued development of techniques for generating multiple alternative interpretations from multimedia data and expanded adversarial evaluations of techniques on synthetic and real-world data.			
Title: Low Resource Languages for Emergent Incidents (LORELEI) ***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 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 status of emerging situations. - Evaluate performance on additional languages, and measure progress on the languages evaluated in the previous year. ***FY 2020 Plans:*** - Implement final improvements and demonstrate capabilities on languages of interest to potential transition sponsors. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 decrease is the result of development work ramping down and focus shifting to technology refinement.	19.201	9.130	4.000
Title: Human-Machine Symbiosis (HMS) ***Description:*** The Human-Machine Symbiosis (HMS) program will conduct applied research 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	-	8.604	16.883

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
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 outcomes; and respond intelligently to new and unforeseen events. A companion basic research effort is funded in PE 0601101E, Project CCS-02. ***FY 2019 Plans:*** - Create human-aligned agent technologies that learn to support individual human operators in the performance of planning tasks. - Devise social Artificial Intelligence (AI) approaches for creating high-performing human-machine teams of individuals and semi-autonomous systems with complementary characteristics/capabilities. - Identify extensions to algorithmic game theory based AI techniques needed for complex military decision problems. - Develop methods for extracting generalized and compressed knowledge representations from data and information to enable more adaptable AI and machine learning approaches. ***FY 2020 Plans:*** - Formulate goal reasoning techniques to serve as the basis for curious machines that identify and fill knowledge gaps. - Design computational agents capable of advising and guiding humans in the performance of real-world tasks. - Develop and demonstrate social AI-based techniques for evaluating and selecting human-machine teams that perform at a higher level than teams constituted using only individual performance assessment techniques. - Incorporate generalized and compressed representations of knowledge in AI and machine learning systems that improve performance on tasks as they gain experience and receive feedback from a human operator. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects expanded work to integrate human-machine symbiosis technologies into a system for assessment.			
Title: Automated Knowledge Acquisition (AKA)	-	-	24.100
Description: The Automated Knowledge Acquisition (AKA) program will develop technologies to automate the integration of diverse sources of data and information into a unified whole. A number of technologies now exist to extract, transform, and load diverse source data into a structured knowledge base. However, each time a new source of data is encountered, a human engineer is required to map that source's metadata and schema to the metadata and schema of the target knowledge base. Performing this mapping is difficult even when design documentation for the source is available, and so it represents a significant barrier to data interoperability and knowledge acquisition. AKA will leverage advances in semantic technology and machine learning to enable machines to perform the entire data integration function without human intervention. AKA technology will automatically learn the semantics of a new data source, characterize source content, align source schema to the target, transform and load values, and reconcile inconsistencies by learning from previously integrated sources. AKA technologies will			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
automatically create and maintain, in real-time, broad knowledge of local and regional military, political, economic, social, and cultural information for warfighters in theater. ***FY 2020 Plans:*** - Apply natural language understanding and machine learning techniques to the problem of automating schema alignment. - Develop approaches for reconciling inconsistencies and assuring integrity of a unified knowledge base created from diverse sources. - Propose an upper ontology to accommodate domain-specific ontologies of interest to military users engaged in human domain operations for which local and regional military, political, economic, social, and cultural factors can be important. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects program initiation.			
Title: Accelerating Artificial Intelligence (AAI) ***Description:*** The Accelerating Artificial Intelligence (AAI) program seeks to go beyond commercially-driven advances in AI and address important national security challenge applications. In particular, this program is focused on improving DoD processes that, because of the need for excessive human involvement, create bottlenecks in DoD's ability to rapidly adapt and deploy new technologies and capabilities. If successful, research efforts under this program will significantly reduce the time and cost associated with many important developmental, approval and certification processes. One technical challenge to be addressed in this program is the need to assess current processes and identify tasks or sub-tasks amenable to minimal human intervention. Other challenges include the need to develop social context aware AI systems and to ensure robustness of AI systems. Approaches to addressing these challenges will leverage recent advances at the frontiers of AI research in transfer learning, causal reasoning and associated models. AAI application areas include the following: (1) machine-enabled techniques to reduce human engagement in determining trustworthiness and intent; (2) automated approaches for accreditation of military software systems; and (3) technologies to restore movement and sensation to central nervous system impaired patients. ***FY 2020 Plans:*** - Evaluate current approaches for assessing trustworthiness and identify tasks or sub-tasks amenable to minimal human intervention. - Apply AI to identify the most effective methods for assessing trustworthiness and intent as a function of social context. - Identify data sources for development and training of AI systems for machine assisted human interviews and vetting processes. - Develop, demonstrate, and evaluate pilot application using algorithmic game theory based AI techniques for complex military decision problems. ***FY 2019 to FY 2020 Increase/Decrease Statement:***	-	-	24.100

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
The FY 2020 increase reflects program initiation.			
Title: Knowledge-directed AI Reasoning Over Schemas (KAIROS)	-	-	15.485
Description: The Knowledge-directed Artificial Intelligence (AI) Reasoning over Schemas (KAIROS) program will develop AI and machine learning technologies to aid a human operator in understanding complex event sequences. For the purposes of KAIROS, an event is an occurrence that results in an observable and recognizable change in either the physical world or human society. Events of particular interest to KAIROS are those that create changes that have significant impact on national or homeland security. Many important events are not simple occurrences but complex phenomena that are composed of numerous subsidiary event elements, some of which happen simultaneously while others are sequential and dependent on each other. Humans make sense of event sequences by organizing them into narrative structures that may occur or re-occur frequently. These structures are abstracted into schemas - organized units of knowledge that represent patterns - for the purpose of cognition. The KAIROS program will develop automated systems that use existing schemas and, when needed, create new schemas to bring structure to complex event sequences and present these structured representations to operators. Given multi-media inputs, operators will use KAIROS technologies to identify subsidiary event elements, determine their temporal order, recognize complex event sequences, and link disparate events. KAIROS technologies will enable analysts and warfighters to understand unfolding events rapidly and accurately. ***FY 2020 Plans:*** - Develop and apply AI and statistical pattern recognition techniques for machine learning of new temporal schemas from intelligence data. - Develop temporal schema to recognize patterns in complex event sequences. - Develop techniques for quantifying the degree to which a temporal schema models a complex sequence of event elements and for quantifying the degree of confidence in reconstructions. - Explore approaches for using partial matches to temporal schema to interpolate or predict missing or future event elements, respectively. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The FY 2020 increase reflects program initiation.			
Accomplishments/Planned Programs Subtotals	69.197	71.864	161.168

	FY 2018	FY 2019
Congressional Add: DARPA Foundational and Applied Artificial Intelligence	-	25.000
FY 2019 Plans: - Define temporal schemas for a broad range of event sequences including in particular events of potential interest to military decision makers.		

Exhibit R-2A, RDT&E Project Justification: PB 2020 Defense Advanced Research Projects Agency		Date: March 2019
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

	FY 2018	FY 2019
- Formulate top-down approaches for associating events under analysis with existing temporal schemas. - Explore approaches that enable adaptation of natural language processing and computer vision technologies to chemistry data.		
Congressional Adds Subtotals	-	25.000

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.