Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Defense Advanced Research Projects Agency	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	-	401.453	428.556	435.920	-	435.920	454.599	467.755	468.030	417.627	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	46.513	16.277	6.576	-	6.576	0.000	0.000	0.000	0.000	-	-
IT-03: *CYBER SECURITY*	-	249.979	251.111	236.182	-	236.182	246.677	257.132	257.043	207.888	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	104.961	161.168	193.162	-	193.162	207.922	210.623	210.987	209.739	-	-

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 2021 Defense Advanced Research Projects Agency	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	404.967	442.556	435.746	-	435.746
Current President's Budget	401.453	428.556	435.920	-	435.920
Total Adjustments	-3.514	-14.000	0.174	-	0.174
• Congressional General Reductions	0.000	-15.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	1.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	5.104	0.000			
• SBIR/STTR Transfer	-8.618	0.000			
• TotalOtherAdjustments	-	-	0.174	-	0.174

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2019	FY 2020
Project: IT-03: *CYBER SECURITY*		
Congressional Add: *Distributed Ledger Technology*	-	1.000
Congressional Add Subtotals for Project: IT-03	-	1.000
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	1.000

Change Summary Explanation

FY 2019: Decrease reflects the SBIR/STTR transfer offset by reprogrammings.
FY 2020: Decrease reflects congressional adjustments.
FY 2021: Increase reflects minor program repricing.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	46.513	16.277	6.576	-	6.576	0.000	0.000	0.000	0.000	-	-

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 will 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, will support new, sustainable computing systems for a broad spectrum of scientific and engineering applications.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: RF Machine Learning Systems (RFMLS)	21.329	16.277	6.576
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 2020 Plans: - Complete final phase development of machine learning algorithms and architectures for two of 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. - Begin technology transition applications.			
FY 2021 Plans: - Complete final phase development of machine learning algorithms and architectures for all of the four challenge problems.			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Complete a real-time, open-air demonstration of RFMLS capabilities. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The decrease in FY 2021 reflects completion of a real-time open-air demonstration of RFMLS capabilities.			
Title: Spectrum Collaboration Challenge (SC2) ***Description:*** The Spectrum Collaboration Challenge (SC2) program catalyzed 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 addressed 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 addressed these challenge by leveraging artificial intelligence and machine learning to optimize use of the spectrum in real-time. In particular, SC2 participants were challenged to develop techniques that allow collaboration among dissimilar communications technologies. SC2 conducted 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.	25.184	-	-
Accomplishments/Planned Programs Subtotals	46.513	16.277	6.576

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	249.979	251.111	236.182	-	236.182	246.677	257.132	257.043	207.888	-	-

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 2019	FY 2020	FY 2021
Title: Memory Optimization (MemOp)	9.500	17.960	19.500

Description: The Memory Optimization (MemOp) program is developing 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 is exploring 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 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 more efficiently, and to accelerate processing pipelines.
- Establish a testbed to evaluate memory transaction improvements in systems incorporating GPUs and FPGAs.
- Begin testing algorithms and architectures for improving memory transaction performance in hardware and software, and evaluate on testbed.

FY 2021 Plans:
- Enhance the scalability of algorithms for task mapping in large scale memory systems, and optimize software implementations.
- Implement and test methods to interface to memory and accelerated processing pipelines.
- Leverage the testbed to evaluate memory transaction improvements in systems incorporating GPUs and FPGAs.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Optimize algorithms and architectures for memory transaction performance in hardware and software, and evaluate on testbed. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects continued development of memory interface methods and accelerated processing pipelines, and expanded use of an enhanced evaluation testbed.			
Title: Cyber-Hunting at Scale (CHASE) ***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 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. - Identify foundational protective measures for adversarial actions such as data exfiltration and lateral movement. - Demonstrate global analysis methods on distributed enterprise networks. ***FY 2021 Plans:*** - Evaluate threat detection, threat characterization, and data planning feedback loops at enterprise scale and demonstrate ability to adapt sensor feeds based on threat characterizations. - Evaluate ability for threat detection and characterization to improve detection accuracy and reduce the time analysts require to diagnose alerts. - Evaluate the extent to which novel data retention policies can improve detection accuracy while reducing the amount of historic data stored. - Quantitatively characterize how the accuracy of global cross-enterprise threat detection depends on data policies. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of development and integration work decreasing, and the focus shifting to demonstration and evaluation on distributed enterprise networks.	20.485	19.000	18.200
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS)	19.000	17.700	15.550

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
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 in networked devices. 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 can 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 aims to enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations. ***FY 2020 Plans:*** - Enhance botnet-tracking algorithms to detect conscripted networks by characterizing botnet management infrastructure. - Expand discovery techniques for additional classes of software vulnerabilities. - Evaluate botnet-tracking algorithms for detecting stealthy command-and-control protocols, and evaluate autonomous agent behavior in contained environments. - Collaborate with transition partners to determine how counter-botnet technologies may be integrated into existing architectures and exercises. ***FY 2021 Plans:*** - Enhance botnet-tracking algorithms to provide near-real-time assessment for the identification and tracking of botnet-conscripted networks. - Expand discovery techniques to address additional platforms and classes of software vulnerabilities. - Evaluate botnet-tracking algorithms for detecting botnet-conscripted networks by characterizing botnet management infrastructure, and evaluate autonomous agent behavior in representative environments. - Collaborate with transition partners to evaluate counter-botnet technology in synthetic environments. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of reduced counter-botnet technology development and prototype integration work, and expanded demonstrations on synthetic environments in collaboration with transition partners.			
Title: Configuration Security ***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 make use of multiple commodity information technology components. The manual configuration necessary to enable each	13.800	14.800	15.207

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
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, ensure secure configuration settings, and prevent malicious changes to these settings. ***FY 2020 Plans:*** - Develop techniques to automatically generate baseline secure configurations for complex 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 2021 Plans:*** - Test and evaluate techniques to automatically generate baseline secure configurations for operationally relevant, complex cyber-physical-human systems, including the translation of human-readable standard operating procedures into machine-understandable formats. - Apply algorithms to automatically reconfigure a critical infrastructure system to a safer and more secure baseline that provides required functionality and supports the new configuration parameter selection with generated human-readable explanations. - Test and evaluate a capability to detect and prevent malicious modification of configurations from the system-generated baseline on a shipboard communications system, and to assist system operators in changing between operational contexts. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects ramping up of algorithm and software development, and expanded demonstrations and evaluation of an automated capability to detect and prevent malicious modification of configurations from the system-generated baseline.			
Title: Computers and Humans Exploring Software Security (CHESS) ***Description:*** 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 mixed-initiative computer-human collaboration. CHESS aims to enable U.S. operational cyber superiority by combining human-generated insight into the vulnerability discovery process with the speed and scale of computational analysis.	13.000	17.500	14.775

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
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. ***FY 2021 Plans:*** - Implement and demonstrate 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. - Expand cyber reasoning techniques to discover additional classes of software vulnerabilities, and enhance representations of information gaps revealed by expanded cyber reasoning techniques. - Demonstrate an end-to-end, integrated computer-human software reasoning system to DoD and Intelligence Community transition partners. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects ramping down of work to integrate technologies in a proof-of-concept, computer-human software reasoning system, and expanded performance assessments on a synthetic challenge corpus.			
Title: Resilient Anonymous Communication for Everyone (RACE)	8.760	12.700	13.900
Description: The Resilient Anonymous Communication for Everyone (RACE) program is developing cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient, mobile communications within a network environment. RACE is developing 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 is based on rigorous security arguments or in statistical arguments based on realistic simulations, and not on ad hoc security claims. ***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 components for a secure message-passing system that can defeat the efforts of a cyber adversary with limited ability to observe the network.			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Develop a testbed that includes representative networks on which to evaluate implementations of the obfuscation and cryptographic technologies and the integrated secure message-passing system against a simulated cyber adversary. ***FY 2021 Plans:*** - Refine and scale up the secure message-passing system by improving the efficiency of techniques for computing on encrypted routing information. - Integrate components into a secure message-passing system to defeat a cyber adversary with limited ability to observe the network by making the communication protocols statistically indistinguishable from legacy protocols. - Enhance the testbed by incorporating an active simulated cyber adversary that seeks to compromise the obfuscation and cryptographic technologies and demonstrate the integrated secure message-passing system. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects expanded development of obfuscation and encryption technologies, continued implementation of a secure message-passing system, and enhancement of a testbed on which to evaluate the system against a simulated cyber adversary.			
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 largely 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. ASED aims to greatly reduce the effectiveness of adversary social engineering attacks and improve the security of DoD information systems. ***FY 2020 Plans:*** - Create the capability to autonomously detect social engineering attacks across multiple communication platforms and to semi-autonomously attribute social engineering attacks. - Develop the capability for multiple, coordinated, counter-social-engineering bots to conduct autonomous investigations of social engineering attacks. - Evaluate effectiveness and efficiency of social engineering detection and investigation techniques. ***FY 2021 Plans:*** - Create the capability to autonomously detect and defend against social engineering attacks across Internet-based communication platforms. - Demonstrate automated attribution of social engineering attacks across multiple communication platforms.	14.524	12.500	10.750

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Assess performance of a bot-based defense system that increases the cost to an adversary of conducting a social engineering attack. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects shift from development of counter-social-engineering bot technologies, to expanded performance assessment across multiple communication platforms.			
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. This 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 is developing 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 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 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 the Defense Information Systems Agency (DISA) and commercial network providers. ***FY 2021 Plans:*** - Increase the operational scale of integrated network-compute elements to thousands of nodes while automatically redistributing workloads. - Optimize and evaluate integrated capabilities over networks with thousands of network-compute elements in terms of the reduction of network bandwidth consumed and the increase in computational utilization.	18.000	16.300	10.200

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Harden, demonstrate, and transition integrated network-compute capabilities to DISA and commercial network providers. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects ramping down of development of the technologies and software prototypes for distributing workloads to network-compute elements, and continuation of testing, demonstration, and transition activities.			
Title: Cyber Assured Systems Engineering (CASE)	21.400	15.100	10.000
Description: The Cyber Assured Systems Engineering (CASE) program is developing the design, analysis and verification tools needed to allow systems engineers to design-in cyber resiliency and manage tradeoffs as they do other quality attributes 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. CASE technologies will enable the design of cyber-physical systems that robustly execute their intended function despite the efforts of sophisticated cyber adversaries. ***FY 2020 Plans:*** - Enhance cyber resilience design tools based on the results of cyber resilience challenge problems. - Apply design tools and techniques to exemplar cyber-physical systems including a military helicopter. - 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 in coordination with potential transition partners and other stakeholders. ***FY 2021 Plans:*** - Enhance cyber resilience design tools based on the results of integrating into the engineering workflow of a defense system provider. - Evaluate and demonstrate design tools and techniques on defense platforms including a military helicopter. - Demonstrate the ability of a defense platform provider to use design tools to produce cyber resilient designs. - Demonstrate enhanced platform cyber resiliency in tests coordinated with potential transition partners and other stakeholders. ***FY 2020 to FY 2021 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
The FY 2021 decrease reflects ramping down of development of techniques and software tools to design-in cyber resiliency requirements, and continued demonstrations on exemplar cyber-physical challenge problems.			
Title: Enhanced Attribution ***Description:*** The Enhanced Attribution program is developing technologies to associate the malicious actions of cyber adversaries with 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 2020 Plans:*** - Integrate new data sets and develop new algorithms to increase resolution from an adversary's infrastructure to an individual actor. - Develop and evaluate predictive analytic algorithms for anticipating adversary actions across a cyber campaign, and adversary pattern matching algorithms for discovering previously unknown campaigns. - Integrate tools and event extraction techniques into an enterprise wide automated attribution platform. - Collaborate with transition partners to test and evaluate the attribution platform's ability to track adversary threat groups. ***FY 2021 Plans:*** - Integrate additional data sources in the attribution platform, and develop techniques for automated and assisted tasking of defensive capabilities. - Adapt tools and techniques to interoperate with existing software frameworks, and extend capabilities of event extraction techniques. - Work with transition partners to evaluate the attribution platform on government-provided data sets and transition the attribution technologies. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects ramping down of development and integration of a prototype platform for attribution, and continued evaluation on government data sets.	20.830	18.100	8.800
Title: Cora ***Description:*** The Cora program is developing 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	7.400	11.000	8.100

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
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 otherwise might not be available. ***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. - Develop natural language processing capability in text-based data other than English. - Create test protocols to evaluate technical progress with respect to automated generation of cyber leads. ***FY 2021 Plans:*** - Implement and evaluate new methods of machine learning for the generation of cyber-specific content. - Implement and evaluate new methods of identifying cyber threats across heterogeneous data, in multiple languages. - Provide initial software capabilities to potential transition partners for performance assessments in operational environments. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects shift from efforts to implement and evaluate an integrated cyber analytical system to transition of technology to operational partners.			
Title: Searchlight	3.800	5.300	6.100
Description: The Searchlight program is developing technologies to ensure that 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 aim to enable organizations to adapt the QoS for their low-priority traffic resulting in improved QoS for their high-priority traffic without affecting traffic from other Internet users. Searchlight technologies will become increasingly important as 5G systems provide advanced capabilities for organizations to adapt their QoS guarantees. ***FY 2020 Plans:*** - Develop a unified framework for network QoS requirements for diverse distributed applications having differing and dynamic priorities. - Implement QoS adaptation schemes on programmable network elements such as software-defined routers and switches. ***FY 2021 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Develop initial implementation of a system integrating automated application inference, network inference, and QoS management. - Evaluate the integrated system in terms of its capability to enable QoS management of heterogeneous distributed applications. - Formulate transition approaches with DoD and commercial network service providers. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects expanded work to integrate QoS adaptation schemes on programmable network elements and to evaluate techniques on heterogeneous distributed applications.			
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	27.310	20.350	5.000
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. RADICS aims to 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 2020 Plans:*** - Provide integrated capability for grid physics anomaly detection and Supervisory Control and Data Acquisition (SCADA) spoofing detection. - Refine secure network communication technologies that optimize the use of available communications links to create ad hoc secure emergency communications networks under conditions of substantial uncertainty. - Demonstrate capabilities to maintain and expand situational awareness in the aftermath of a cyber-enabled attack on the power grid. - Evaluate capability for rapid localization, isolation, and characterization of cyber weapons targeting a wide range of industrial control system devices and networks, and develop automated approaches to support cyber first responders in remediation efforts. - Collaborate with private industry, DoE, and other USG organizations to conduct robust exercises demonstrating enhanced capabilities to support black start restoration of a power grid amidst a cyber attack, and transition technologies. ***FY 2021 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Harden demonstrated capabilities to maintain and expand situational awareness in the aftermath of a cyber-enabled attack on the power grid in response to utility company feedback. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 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: Intent-Defined Adaptive Software (IDAS) ***Description:*** The Intent-Defined Adaptive Software (IDAS) program, addressing issues encountered in the Cyber Assured Systems Engineering (CASE) program, budgeted within this PE and Project, will develop technologies to represent the intent of software and its abstract constraints separately from its concrete instantiation, for the purpose of enabling rapid code synthesis and continual adaptation. Modern weapons platforms are increasingly dependent on complex software, increasing the risk of system failures and creating new attack surfaces for adversaries. Software engineers often manage complexity by choosing a particular option that fulfills the immediate needs of the development effort, e.g., by concretization. IDAS will develop techniques for deferring software concretizations until uncertainties are resolved, either at build time or during run time, for complex systems. IDAS technology aims to significantly reduce software development time and maintenance costs, thereby enabling DoD to acquire, sustain, and improve software-based capabilities more cost-effectively. ***FY 2020 Plans:*** - Formulate novel software engineering approaches that create and enforce strict separation between an abstract problem, including goals, constraints, and preferences, and concrete implementations. - Explore alternative approaches for automating the synthesis of code given its intent, quality goals, and operational constraints. - Develop an approach for using formal methods to verify that synthesized implementations will respect the goals and constraints of the problem. ***FY 2021 Plans:*** - Develop algorithms for deferring software concretizations until uncertainties are resolved for complex systems. - Develop techniques that permit optimization of multiple implementations, and enable more efficient encoding of quality goals and operational constraints. - Implement alternative software synthesis algorithms for automated modification by revising the representation of the intent of the software. ***FY 2020 to FY 2021 Increase/Decrease Statement:***	-	8.000	17.400

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
The FY 2021 increase reflects ramping up of development of techniques for deferring software concretization and initial implementation of alternative synthesis algorithms.			
Title: Assured Micropatching (AMP)	-	7.100	16.800
Description: The Assured Micropatching (AMP) program, building on technical challenges encountered in the Computers and Humans Exploring Software Security (CHESS) program, also budgeted in this PE and Project, will develop technologies to enable the rapid production of targeted micropatches to repair legacy program binaries with strong guarantees. At present, the emergency patching of legacy software, even if all relevant information is available, takes far too long, leaving critical systems with known flaws vulnerable to adversary attack. AMP will create the capability to analyze, modify, and fix legacy software in binary form even when the original source code and/or build process is not fully available. The AMP technical approach involves automatic discovery of known vulnerable components, goal-driven decompilation to isolate and analyze the vulnerable binary components, and minimal-change patching and recompilation to rebuild affected binaries with strong guarantees that the patch will not impair the functions of the system. The technologies developed by AMP aim to enable cyber defenders to quickly and accurately patch legacy binaries in the deployed software systems upon which our military depends. ***FY 2020 Plans:*** - Devise approaches for decompiling binary programs that can meet objectives such as alignment with available source code or fitness for a specified task. - Formulate strategies for producing a binary patch that is minimal with respect to the original binary when recompiled, with strong guarantees that the patch will not impair the functions of the system. - Design challenge tests for evaluating binary micropatching capabilities including challenges involving heavy vehicle firmware and other embedded and military systems. ***FY 2021 Plans:*** - Develop prototype goal-driven decompilers, and demonstrate feasibility of iteratively guiding decompilation with fitness functions relevant to repairing binary flaws. - Develop prototype recompilers that produce both a micropatch and a formal representation of the effects of the micropatch suitable for use in a proof that the effects of the patch are isolated from other components. - Perform initial tests of decompiler and recompiler prototypes on at-scale system binaries. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects a shift from initial designs to developing prototype decompilers and recompilers.			
Title: Securing Information for Encrypted Verification and Evaluation (SIEVE)	-	7.700	14.900

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
Description: The Securing Information for Encrypted Verification and Evaluation (SIEVE) program, expanding on technical opportunities discovered in the Brandeis program, budgeted within this PE and Project, will develop technology to enable creation of mathematically verifiable public statements derived from sensitive information that remains hidden. To accomplish this, SIEVE will produce advances in a cryptographic technique known as zero knowledge (ZK) proofs, which simultaneously enable mathematical verification of public statements while provably hiding the sensitive information from which the statement is derived. The advances produced by SIEVE will make it possible to verify statements substantially more complex than the current ZK state of the art supports, for example, statements about a software vulnerability that do not reveal details of how the vulnerability can be exploited. ***FY 2020 Plans:*** - Build efficient ZK proof generation compilers optimized for large and complex problem statements, and that can operate in an efficient manner. - Explore asymptotically efficient ZK constructions in the post-quantum setting. - Develop methodology to validate the functionality of ZK techniques and software on a set of possible DoD applications. ***FY 2021 Plans:*** - Extend ZK proof generation compilers to permit optimization for any subset of prover computation, verifier computation, total communication, and total number of communication rounds. - Extend post-quantum analyses to important cases such as non-interactive zero knowledge from post-quantum assumptions and zero knowledge from symmetric key primitives. - Validate the functionality, information leakage potential, and robustness to attack of developed ZK techniques and software on a set of DoD relevant applications. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects expanded development work to extend cryptographic technologies and to validate their functionality, information leakage potential, and robustness to attack on a set of possible DoD applications.			
Title: Fast Network Interface Cards (FastNICs) ***Description:*** The Fast Network Interface Cards (FastNICs) program, expanding on technical opportunities discovered in the Dispersed Computing program, budgeted within this PE and Project, will create new networking technologies to accelerate the computation of distributed applications. Today's network and computing subsystems are badly out of balance with each other, a result of incremental technology advances in networking and computing market silos. This has produced a bottleneck at the network interface used to connect a machine to an external network, severely limiting the input/output capability. FastNICs will develop new input/output technologies based on more realistic models of complex multiprocessor compute, interconnect, and	-	6.500	13.900

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
memory subsystems. FastNICs aims to enable a dramatic increase in computational throughput for distributed applications such as iterative training of machine learning systems. ***FY 2020 Plans:*** - Design improved architectures for the interface between an external network and a computing system that better balance communications bandwidth and processing throughput. - Extend the most widely used distributed systems software and operating systems to accommodate massively parallel input data streams. - Design algorithms and software for distributed computing applications, such as machine learning, that effectively utilize massively parallel data streams. ***FY 2021 Plans:*** - Implement and evaluate alternative architectures for the network interface, and quantify achievable communications bandwidth and processing throughput. - Demonstrate versions of widely used distributed systems software and operating systems that accommodate massively parallel input data streams. - Implement distributed computing applications, such as machine learning, that effectively utilize massively parallel data streams, and demonstrate performance improvements. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects expanded work to implement improved network interfaces and to demonstrate the technology on important distributed applications.			
Title: Open, Programmable, Secure 5G (OPS-5G) ***Description:*** The Open, Programmable, Secure 5G (OPS-5G) program, addressing key technical issues explored in the Searchlight program (also budgeted in this PE and Project) will develop open source, 5G network software that ensures security and stimulates innovation in mobile wireless hardware. Current trends in mobile wireless technology development are unfavorable in that the U.S. is increasingly dependent on proprietary technologies offered by foreign suppliers. OPS-5G will develop standards-compliant software for 5G mobile wireless networks that is open source, programmable, and secure by design. The availability of open source software for 5G will have the additional benefit of opening the mobile wireless hardware market to new participants, stimulating innovation and competition. The OPS-5G program aims to move the mobile wireless market off its current model of opaque, proprietary, and vertically-integrated technology provided by a small number of dominant vendors to a more robust model of transparent, open source technology created by a diverse ecosystem of academic and commercial software and hardware developers. OPS-5G will be coordinated with existing open-source 5G efforts and USG stakeholders.	-	-	12.100

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
FY 2021 Plans: - Formulate approaches for addressing 5G security challenges, such as eavesdropping at access points, and denial of service. - Formulate approaches for automatically extracting information relevant to software implementations including software structure, service interfaces, timing parameters, flow diagrams, and protocol graphs from 5G standards maintained in electronic documents. - Formulate 5G node and network security architectures, and initiate development of tools for integrity checks, prevention, remote diagnosis and recovery. - Devise in-network sensors and reactive defenses for onset detection and scalable resilience against distributed denial of service (DDoS) attacks in 5G networks. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects program initiation.			
Title: Cyber Course of Action Analysis (C2A2) ***Description:*** The Cyber Course of Action Analysis (C2A2) program will develop technologies for automatically generating and analyzing cyber courses of action (COAs) represented as graph structures. At present, developing cyber COAs to achieve specified effects, and assessing the risks associated with these COAs, is largely a manual process requiring many hours of effort. C2A2 aims to enable U.S. cyber operators to conduct cyber operations more rapidly and with greater degrees of success. ***FY 2021 Plans:*** - Develop analyst interface to enable automated cyber report generation. - Evaluate the utility of the interface and reports for quantifying the risk of cyber operations. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects program initiation.	-	-	5.000
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 by advantageously 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, 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 2020 Plans:***	15.300	10.981	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Explore distance versus accuracy tradeoffs for discriminating between known and 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 complex devices, including those with field programmable gate arrays. - Support potential transition partners in test and evaluation using complex devices operating in both correct and compromised states. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of program completion.			
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 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 data communication privacy protection in 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 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of program completion.	18.870	6.520	-
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 conscript poorly defended IoT devices into	10.000	5.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
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 2020 Plans:*** - Finalize testing and verification of the prototype defensive architectures by subjecting techniques to simulated DDoS attacks. - Harden, demonstrate, and transition technologies to the Defense Information Systems Agency (DISA) and commercial network providers. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of program completion.			
Title: Cyber Fault-tolerant Attack Recovery (CFAR) ***Description:*** The Cyber Fault-tolerant Attack Recovery (CFAR) program developed 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 combined 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 can quickly detect deviations in processing elements at attack onset and rapidly reboot to restore affected services. CFAR technologies were developed in coordination with operational users.	5.000	-	-
Title: Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) ***Description:*** The Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) program developed 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 against network infrastructure. EdgeCT technologies were developed in coordination with operational commands and commercial service providers.	3.000	-	-
Accomplishments/Planned Programs Subtotals	249.979	250.111	236.182

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

	FY 2019	FY 2020
Congressional Add: Distributed Ledger Technology ***FY 2020 Plans:*** - Conduct research in distributed ledger technology.	-	1.000
Congressional Adds Subtotals	-	1.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	104.961	161.168	193.162	-	193.162	207.922	210.623	210.987	209.739	-	-

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; software developers and certifiers to design, implement, evaluate, and accredit cyber-physical systems with greater efficiency and confidence; 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 2019	FY 2020	FY 2021
Title: Symbiotic Design*	10.701	16.883	23.582
Description: *Formerly Human-Machine Symbiosis (HMS) The Symbiotic Design program is developing artificial intelligence-based approaches to augment human teams in the design of cyber-physical systems (CPS), and thereby significantly reduce time to deployment. The current generation of DoD systems and platforms integrate cyber and physical subsystems. The capability of the engineering teams has not scaled with the enormous complexity of modern CPS. Engineering organizations require large teams of engineers that collectively possess the necessary domain knowledge (of component technologies, theories, and tools), but the prolonged timelines of the development process for modern CPS hinders DoD's ability to counter emerging threats. The Symbiotic Design program will address this challenge by transforming the human-focused, model-based design flows used today into a symbiotic process of collaborative discovery by humans and continuously-learning AI-based co-designers. The program will create technologies essential for AI co-design, notably design space construction, design composition, and design space exploration. The program will demonstrate the approach at realistic scales by a sequence of CPS design challenges of increasing complexity, and quantify the results with respect to development time, system performance, and innovation metrics.			
FY 2020 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Explore alternative means for human designers to communicate design intent via domain-specific design artifacts such as seed designs, design fragments, or abstract designs, in addition to traditional specifications such as performance and functional objectives. - Formulate approaches by which an AI co-designer can learn from past successful designs to propose new designs and refinement alternatives. - Introduce techniques for defining design spaces and for evaluating design points using domain-specific analysis and simulation tools. ***FY 2021 Plans:*** - Develop prototype mining engines and feature extractors to enable query generation from seed designs and extract heterogeneous model-based design artifacts. - Develop techniques for exploring high-dimensional, multi-domain, combinatorial design spaces and design elaboration methods for automated model completion by an AI co-designer across multiple design domains. - Produce design challenge problems, and evaluate the effectiveness of symbiotic design technologies on sub-systems and systems of interest to the DoD. - Incorporate learning capabilities in computational agents that offer personalized guidance and anticipate the specific needs of each individual user. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects ramping up of development and implementation of symbiotic design techniques and evaluation on systems of interest to DoD.			
Title: Assured Autonomy	19.520	25.550	19.000
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, 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 2020 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Develop scalable methods addressing formal verification of a preliminary set of safety properties for 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 that diverge from 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 2021 Plans:*** - Integrate learning-enabled components with examples of formally verified safety properties into autonomous systems, and implement scalable algorithms for dynamic evaluation of assurance cases. - Develop and evaluate scalable monitoring techniques to detect data-distribution shifts on simulated and real-world data in which the operating environment diverges from the training environment. - Develop scalable techniques for runtime verification of learning-enabled systems, and integrate safety constraints in online learning algorithms. - Demonstrate technologies on assurance challenge problems for several learning-enabled autonomous platforms of interest to the DoD. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects a shift from development efforts to technologies being demonstrated on several learning-enabled autonomous platforms.			
Title: Active Interpretation of Disparate Alternatives (AIDA)	19.780	25.000	18.600
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 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 insufficient interpretations because alternatives are 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 diverse media into a common semantic representation, aggregate information, resolve ambiguities, discover conflicting information, and generate and explore multiple interpretations of events, situations, and trends. AIDA aims to provide decision makers a capability to understand alternative explanations for available information and to make contingency plans accordingly. ***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.			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Develop an intuitive interface that allows users to modify the extracted semantic elements and 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 2021 Plans:*** - Develop the means to rank hypotheses according to relevance and confidence, and the capability to verify and explore hypotheses injected by users. - Enhance the capability of the system to infer components of hypotheses not explicit in the input. - Enhance the interface to facilitate the capability of the user to refine the extracted semantic elements and the generated hypotheses. - Collaborate with transition partners to conduct experiments to evaluate performance on operational data. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects ramping down of development of techniques for generating multiple alternative interpretations from multimedia data, and continued evaluations of techniques on synthetic and real-world data.			
Title: Explainable Artificial Intelligence (XAI)	20.830	26.050	17.380
Description: The Explainable Artificial Intelligence (XAI) program is developing a new generation of machine learning techniques that are able to explain their rationale, characterize their strengths and weaknesses, and convey an understanding of how they will behave in the future. AI is a critical enabler for U.S. military systems that will perform increasingly complex and sensitive missions. 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, not meaningful to a human user, or inconsistent with the full range of behaviors of the AI system. 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 that are meaningful to end-users. XAI implementations will be developed and demonstrated in next-generation data analytics and autonomous systems. ***FY 2020 Plans:*** - Refine the cognitive model of explanation, and show increased effectiveness of explanations generated by the systems. - Optimize explainable machine learning techniques and user interfaces for integration into prototype systems. - Expand the set of test problems in data analytics and autonomy for evaluating performance, explanation accuracy, and effectiveness of the systems.			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Evaluate performance and explanation effectiveness against test problems in data analytics and autonomy. ***FY 2021 Plans:*** - Enhance explainable systems for robustness to increased machine learning task complexity. - Expand the cognitive model of explanation based on task performance evaluations with operational users. - Measure system explainability, accuracy, and learning performance against additional datasets and scenarios. - Select and integrate subsets of explainable model techniques in an operational prototype system for capability demonstrations coordinated with DoD and Intelligence Community (IC) partners. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease reflects ramping down of development of explainable machine learning techniques, continued integration of techniques in machine learning systems, and expanded testing on problems in data analytics and autonomous systems.			
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 human-AI collaborations to mitigate current bottlenecks in DoD's ability to rapidly adapt and deploy new technologies and capabilities. If successful, research efforts under this program will significantly accelerate the pace of innovation in many important DoD domains while also reducing the time and cost associated with approval and certification processes needed to transition and deploy new technologies. One technical challenge to be addressed in this program is the need to assess current developmental, approval, and certification processes and identify tasks or sub-tasks amenable to greater automation with minimal human intervention. Other challenges include the need to develop social context aware AI systems and to ensure robustness of AI systems, particularly in novel and/or unanticipated situations. 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 efficiently capture, generate, and analyze disparate data sources to accelerate design and development of new materials and chemistries for DoD specific applications; (2) knowledge management tools that can efficiently capture, analyze and reason with expertise, experience, and data to prevent loss and increase value of critical national security knowledge/expertise; and (3) social context informed AI approaches to enable reliable and robust forecasting and decision aiding tools for stabilization, deterrence and gray zone operations. ***FY 2020 Plans:*** - Identify technical and programmatic criteria for military applications for testing and evaluating novelty-aware AI technologies. - Establish evaluation criteria and effective performance goals for novelty aware AI technologies in real military AI applications. - Identify data sources for development and training of AI systems for machine assisted human interviews and vetting processes.	-	24.100	29.400

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
- Develop, demonstrate, and evaluate pilot applications using algorithmic game theory based AI techniques for complex military decision problems. - Perform initial assessment of data, tools, and models associated with molecular design systems for relevance to DoD applications. - Develop and test AI system capabilities to provide plausible counterfactual predictions as evidence of AI contextual reasoning. - Develop sensing theories and concepts with a focus on information-shaping, data security, and personal privacy. - Implement prototype test bench systems, using commercial of the shelf (COTS) Field-Programmable Gate Array, photonic, and electronic components, to demonstrate the real-world system/process of the targeted signature detection applications. - Develop techniques to implement shallow neural networks (SNNs) with a non-multiply-accumulate based compute primitive. - Demonstrate a 10x reduction in SNN parameters with accuracy comparable to state of the art deep neural networks. - Develop and demonstrate algorithms that show progress towards enabling computers to learn real world concepts expressed in natural language, based on our understanding of how children learn language focusing on naming of visible objects and their attributes. - Demonstrate benchtop SNN in a DoD relevant communications or sensing application for edge AI, and performance projections of the SNN to a custom digital integrated circuit. - Develop adaptive signal processing kernels based on physics models and use generative training to improve accuracy of neural network kernels. - Implement a reconfigurable kernel toolkit for application development in either a communications or RADAR based suite to achieve 10x improvement in the system performance of input signal-to-noise sensitivity or signal-to-interference rejection ratio. - Determine extensibility and limitations of the approach by implementing the methodology and second game of different type/ architecture. - Develop and exercise exploration architectures including mission ontologies for representing contextual knowledge necessary to address primary research questions. Research questions center around machine teaming methods, especially decentralized heterogeneous machine teaming. - Initiate efforts to accelerate Artificial Intelligence with a focus on third wave AI.			
FY 2021 Plans: - Select military application(s) into which to insert and evaluate novelty-aware AI technologies. - Initiate transition of novelty generation technologies from research domains to military application domains. - Validate process and property optimization capabilities of molecular design systems through challenges informed by DoD applications. - Commence development of information-shaping sensor prototypes to validate privacy-assured sensing concepts. - Continue efforts to accelerate Artificial Intelligence with a focus on third wave AI.			
FY 2020 to FY 2021 Increase/Decrease Statement:			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
FY 2021 increase reflects a shift from initial planning and exploration to system development.			
Title: Automated Rapid Certification Of Software (ARCOS)*	-	24.100	27.000
Description: *Formerly Automated Knowledge Acquisition (AKA) The Automated Rapid Certification of Software (ARCOS) program is developing technologies that automate the evaluation of software assurance evidence to enable certifiers to determine earlier in the process that system risks are acceptable. Current software certification practices do not scale with the amount of software being deployed by the DoD, so certification is becoming a bottleneck to new system deployment. ARCOS technologies will address DoD software system certification time and cost. ARCOS technology will automatically generate strong assurance arguments that incorporate supporting evidence for certification criteria. ARCOS will also develop techniques to compose assurance arguments for pre-evaluated components into consolidated assurance arguments for new systems incorporating those components. ***FY 2020 Plans:*** - Design languages and tools for generating assurance case arguments suitable for integration in software development environments. - Develop techniques for extracting a model or specification of legacy software, and for analyzing the legacy assurance evidence. - Develop techniques for integrating diverse assurance evidence within a single structured representation. - Architect approaches for automatically generating and validating assurance case arguments and calculating their confidence level. ***FY 2021 Plans:*** - Extend assurance-case engineering tools to facilitate the design and implementation of software and associated assurance evidence. - Develop approaches to analyze legacy software assurance evidence and specifications to determine areas of insufficient assurance. - Scale data structure representations to accommodate assurance evidence from complex military platforms. - Demonstrate and validate automatically-generated assurance case arguments. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects ramping up of development of assurance case engineering tools, and demonstration of techniques on evidence from representative military platforms.			
Title: Knowledge-directed AI Reasoning Over Schemas (KAIROS)	-	15.485	21.000

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
Description: The Knowledge-directed Artificial Intelligence (AI) Reasoning over Schemas (KAIROS) program is developing AI and machine learning technologies to aid a human operator in understanding complex sequences of events in the world. 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. The KAIROS program will develop automated systems that use existing event-representation 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 aim to enable analysts and warfighters to understand unfolding events rapidly and accurately. ***FY 2020 Plans:*** - Develop and apply AI techniques for automated learning of new schemas for simple and complex events from open source data. - Develop temporal schemas 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 those models. - Explore approaches for using partial matches to temporal schemas to interpolate or predict missing or future event elements. ***FY 2021 Plans:*** - Develop and assess the capability for machine learning of complex schemas from large multimedia data sets. - Develop and evaluate the capability for matching unfiltered simple events from unconstrained large data sets to an initial schema library. - Develop and assess machine learning classifiers for categorizing the temporal and causal relationship between two simple events that are part of a complex event sequence. - In collaboration with potential transition partners, establish thresholds for mission utility for anticipating future events that are part of partially-observed complex events in operational data. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects ramping up of development of techniques for learning complex schemas, and initiation of assessment of techniques on operational data.			
Title: Stylized Language Processing (SLP)	-	-	20.000
Description: The Stylized Language Processing (SLP) program will develop automated language processing techniques for sources that exhibit high degrees of domain-specific specialization. Natural language processing (NLP), a venerable sub-field of AI, has produced advanced but inexact capabilities for computers to process, translate, capture, transform, and utilize the			

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
information contained in the text and speech humans use for their everyday communications. Highly stylized language, for which standard NLP is dubitable, has been encountered in new language genres such as the language intrinsic to social media, for which style may be so heavy as to resemble a code. Importantly, stylized language in a constrained form is also characteristic of technical, legal, scientific, and other more formal sources encountered in specialized domains. Finally, the challenges that arise from language manifestations as influenced by culture, emotion, and media choice provide further motivation for language processing capabilities that exploit features of style. These cases challenge standard NLP but also offer opportunities for greater accuracy. The SLP program will develop language processing technologies for stylized language as it is used in specialized domains, new communication and social media, and by diverse cultures and populations. The techniques developed under the SLP program will be coordinated with DoD operators and applied to military application areas such as the engineering development of complex systems and intelligence analysis of foreign language information in cultural context. ***FY 2021 Plans:*** - Formulate automated techniques to process, translate, capture, transform, and utilize the information contained in technical, legal, scientific, and/or other stylized sources encountered in specialized domains. - Formulate automated techniques for understanding language manifestations as influenced by culture, emotion, and media choice. - Formulate initial applications of stylized language processing technologies to military application areas such as the engineering development of complex systems and intelligence analysis of foreign language information in cultural context. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects program initiation.			
Title: Engineering Artificial Intelligence Systems Implementations (EAISI)	-	-	17.200
Description: The Engineering Artificial Intelligence Systems Implementations (EAISI) program will create technologies and tools to support the development of viable and trusted system that include AI and machine learning (ML) capabilities. Modern AI-dependent systems may include multiple AI components, drawing on a diverse set of AI-related techniques, ranging from machine learning (ML) to knowledge representation, search, planning, game theory, and optimization. Current methods for development of such systems remains primarily based on trial-and-error designs, with limited abstractions, architectures, and patterns. These developments can be costly, risky, and demanding of very high levels of expertise. To address this, EAISI researchers will develop abstractions, patterns, architectures, assurance techniques, and iterative processes that facilitate the analysis and synthesis of complex systems that must rely on AI-based components and associated training data. One of the more difficult engineering challenges with AI is evaluation and assurance, since AI-based systems tend to resist traditional approaches to testing, inspection, and analysis. It is not possible to fully test an AI-based system for every situation it will ever encounter, so new techniques are needed for verifying and validating AI-based systems. EAISI aims to create software and systems engineering			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020	FY 2021
techniques, tools, and practices to facilitate the development of AI-based systems that are capable, trustworthy, affordable, and timely. ***FY 2021 Plans:*** - Formulate rigorous approaches for managing training data for AI-based systems, including provenance, security, and quality, in the engineering of an AI-based system. - Devise approaches for testing, analyzing, and evaluating AI-based systems as means for gaining confidence in and validating those systems. - Initiate the implementation of AI engineering technologies into tools for use by non-expert developers and evaluators. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 increase reflects program initiation.			
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, which are languages for which few linguists are available and automated human language technologies do not exist. 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 are targeted capabilities that 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 2020 Plans:*** - Implement final improvements, and demonstrate capabilities on languages of interest to potential transition sponsors. - Integrate the situational awareness platform into the work space of transition partners, and support field tests. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The FY 2021 decrease is the result of program completion.	9.130	4.000	-
Accomplishments/Planned Programs Subtotals	79.961	161.168	193.162

	FY 2019	FY 2020
Congressional Add: DARPA Foundational and Applied Artificial Intelligence	25.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Advanced Research Projects Agency		Date: February 2020
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 2019	FY 2020
FY 2019 Accomplishments: - Defined temporal schemas for a broad range of event sequences including in particular events of potential interest to military decision makers. - Formulated top-down approaches for associating events under analysis with existing temporal schemas. - Developed approaches for integrating and enforcing safety constraints in learning-enabled systems. - Enabled natural language learning as a child would, based on visual cues gleaned from events, objects, and their properties. - Initiated effort to develop AI systems that can leverage disparate data sources for counterfactual reasoning and prediction. - Implemented comprehensive photonic reservoir algorithms, architectures and hardware for the performance requirements of targeted signature detection applications. - Investigated next-generation AI technologies to develop long-lasting, high-bandwidth neural prosthetics.		
Congressional Adds Subtotals	25.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A