Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Defense Advanced Research Projects Agency	Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
Total Program Element	-	405.789	480.363	388.270	-	388.270	377.426	352.139	372.784	379.890	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	14.710	25.000	11.250	-	11.250	15.000	18.750	15.000	15.000	-	-
IT-03: *CYBER SECURITY*	-	240.074	252.089	183.786	-	183.786	158.669	130.205	128.157	135.353	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	151.005	203.274	193.234	-	193.234	203.757	203.184	229.627	229.537	-	-

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. This Program Element also supports innovation and robust transition planning in the technology cycle by working with entrepreneurs to increase the likelihood that DARPA funded technologies take root in the U.S. and provide new capabilities for national defense.

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, artificial intelligence, and quantum computing, and to maintain the security of DoD information systems. The project therefore aims not only to create new computing platforms to include quantum technology, 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 for 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.

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.

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;

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Defense Advanced Research Projects Agency	Date: April 2022
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*

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 and other complex software-reliant 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. Program Change Summary ($ in Millions)	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total
Previous President's Budget	420.920	430.363	0.000	-	0.000
Current President's Budget	405.789	480.363	388.270	-	388.270
Total Adjustments	-15.131	50.000	388.270	-	388.270
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	50.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	-1.578	0.000			
• SBIR/STTR Transfer	-13.553	0.000			
• Adjustments to Budget Year	-	-	388.270	-	388.270

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2021	FY 2022
Project: IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*		
Congressional Add: *Quantum Computing Acceleration - Congressional Add*	-	25.000
Congressional Add Subtotals for Project: IT-02	-	25.000
Project: IT-03: *CYBER SECURITY*		
Congressional Add: *AI Cyber Data Analytics (Cyber) - Congressional Add*	-	15.000
Congressional Add Subtotals for Project: IT-03	-	15.000
Project: IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*		
Congressional Add: *AI Cyber Data Analytics (AI) - Congressional Add*	-	10.000
Congressional Add Subtotals for Project: IT-04	-	10.000

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Defense Advanced Research Projects Agency	Date: April 2022
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*

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2021	FY 2022
Congressional Add Totals for all Projects	-	50.000

Change Summary Explanation

FY 2021: Decrease reflects reprogrammings and SBIR/STTR transfer.
FY 2022: Increase reflects Congressional adds for Quantum Computing Acceleration and AI, Cyber, Data Analytics.
FY 2023: FY 2023 funding increase reflects the fact that the FY 2022 President's Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	14.710	25.000	11.250	-	11.250	15.000	18.750	15.000	15.000	-	-

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, artificial intelligence, and quantum computing, and to maintain the security of DoD information systems. The project therefore aims not only to create new computing platforms to include quantum technology, 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 for 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 2021	FY 2022	FY 2023
Title: RF Machine Learning Systems (RFMLS) ***Description:*** The RF Machine Learning Systems (RFMLS) program addressed the performance limitations of conventional radio frequency (RF) systems such as radar, signals intelligence, electronic warfare, and communications. The objective of the RFMLS program was to both develop these foundational technologies and to apply them to relevant DoD systems.	14.710	-	-
Title: Underexplored Systems for Utility-Scale Quantum Computing (US2QC) ***Description:*** It has been credibly hypothesized - but not proven - that a fault-tolerant quantum computer of sufficient size would revolutionize multiple commercial industries and scientific disciplines. It is currently expected that this type of machine will not be realized for at least 10 years and as long as 40 years. As a result, the unexpected and near-term development of a scalable, fault-tolerant quantum computer represents a strategic surprise for the United States. In addition, if quantum computers are shown to have transformative potential for critical problems facing the United States, it is in the Government's interest to foster and accelerate commercial progress towards a truly useful, "utility-scale" quantum computer. Initiated under Alternative Computing to both reduce strategic risk and realize transformative opportunity, the US2QC thrust will (1) evaluate disruptive designs for utility-scale, fault-tolerant quantum computers, specifically, systems that can be constructed in less than 10 years; (2) demonstrate each of the enabling sub-systems and components for these designs; and (3) construct a prototype fault-tolerant quantum computer that demonstrates that utility-scale design is viable.	-	-	11.250

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
FY 2023 Plans: - Evaluate system engineering point designs for at least one approach to building a fault-tolerant quantum computer. - Continue development of a testing and evaluation framework to determine if a disruptive approach to building a fault-tolerant quantum computer can succeed within a near-term timeframe. - Create a testing and evaluation framework for the critical components and sub-systems required to achieve utility-scale quantum computing within a near-term timeframe. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY2023 increase reflects program initiation.			
Accomplishments/Planned Programs Subtotals	14.710	-	11.250

	FY 2021	FY 2022
Congressional Add: Quantum Computing Acceleration - Congressional Add	-	25.000
FY 2022 Plans: - Accelerate efforts to verify and validate at least one approach to fault-tolerant quantum computing. - Initiate efforts to create a testing and evaluation framework to evaluate system designs for approaches to building a fault-tolerant quantum computer within the near-term. - Initiate government-driven applications exploration for utility-scale quantum computing, with the eventual goal of developing better metrics for verification and validation.		
Congressional Adds Subtotals	-	25.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	240.074	252.089	183.786	-	183.786	158.669	130.205	128.157	135.353	-	-

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 existing and 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 2021	FY 2022	FY 2023
Title: Open, Programmable, Secure 5G (OPS-5G)	13.300	21.000	28.300
Description: The Open, Programmable, Secure 5G (OPS-5G) program is developing 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. and allies are 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 with increased transparency and 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 U.S. Government, DoD, and industry stakeholders. ***FY 2022 Plans:*** - Implement and evaluate prototype systems that address 5G security challenges, such as eavesdropping at access points and denial of service. - Implement and evaluate prototype software for automatically extracting information relevant to software implementations including software structure, service interfaces, timing parameters, flow diagrams, and protocol graphs from electronic 5G standards. - Implement, evaluate, and demonstrate 5G node and network security technologies and tools for integrity checks, attack prevention, remote diagnosis, and service recovery.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Assess and develop information protection techniques suitable for current and future mobile wireless systems to support DoD operational security needs. ***FY 2023 Plans:*** - Develop and evaluate security architectures capable of defending Internet-of-Things-class devices with low size, weight, and power characteristics. - Scale programmability-based network defenses to handle large-scale distributed denial-of-service attacks. - Deploy and evaluate security architectures on multiple DoD sites, and demonstrate secure voice call capabilities over untrusted network nodes to commercial vendors and service providers, the DoD, and other U.S. Government stakeholders. - Test and validate integrated information protection techniques suitable for current and future mobile wireless systems to support DoD operational security needs. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects ramping up of development and implementation of 5G network security technologies, and expanded demonstration and evaluation in collaboration with industry, DoD, and U.S. Government stakeholders.			
Title: Program Analysis for Capability Excellence (PACE)	10.400	19.250	23.000
Description: The Program Analysis for Capability Excellence (PACE) program will develop tools and techniques to autonomously identify adversary compromise of software, mitigate negative effects of adversary capabilities, and restore the integrity of compromised software. PACE will enable rapid, autonomous response to cyber attacks without using source code or requiring recompilation. ***FY 2022 Plans:*** - Implement emerging software compromise identification and mitigation techniques in an initial proof-of-concept autonomous system. - Demonstrate techniques for attack-specific mitigations that can be rapidly generated and deployed with minimal human assistance. - Assess autonomous system performance against synthetic attacks representative of real world threats. ***FY 2023 Plans:*** - Develop a system to identify and mitigate software compromise for a range of technical targets of increasing complexity. - Demonstrate the autonomy of the system by increasing the scale of software under attack and the sophistication of the simulated attacker. - Assess autonomous system performance against real-world attacks, including both automated adversaries and human experts. ***FY 2022 to FY 2023 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
The FY 2023 increase reflects continued development of techniques for autonomously identifying and mitigating compromise and expanded efforts related to implementation and assessment.			
Title: Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)	9.800	14.750	19.000
Description: The Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS) program is creating methods and tools to recover succinct models of domain data abstractions and logic from source code, add enhancements to the models, and convert them to performant new component implementations verified to be compatible and secure. DoD has a critical need for replacing or reworking components of existing software with more secure and more performant code, including cases where a key performance or security benefit comes from moving parts of the software to new hardware, such as utilizing hardware accelerators, isolation enclaves, offload processors, and distributed computation. However, at present, enhancing legacy software components faces high risk that the new software will not be fully compatible with the existing larger environment. Moreover, verified software is currently written from scratch, starting with a formal specification, rather than incrementally added to a system as provably compatible enhancements. V-SPELLS will address these problems by combining novel concepts in verified programming with recent developments in domain specific languages (DSLs) and systems architecture. V-SPELLS aims to enable piecewise, compatible-by-construction improvement of software components in legacy DoD systems, providing to incremental software (re)engineering the benefits of formal software verification currently available only to clean-slate development efforts. ***FY 2022 Plans:*** - Implement automated techniques for decomposing legacy code into functional modules with domain data structure and operation definitions, untangling of legacy code into low-level domain operation implementations and higher-level application logic, and lifting of legacy code into an extracted DSL. - Develop and formally ground software compartmentalization techniques for subdividing software systems into isolated compartments with limited interconnections intended to minimize privilege and thereby mitigate the impact of software compromise. - Create an initial development environment for convergent DSL programming, including compatibility-centric program analysis techniques that provide efficient, intelligible feedback and refined counterexamples to developers. - Identify DoD software environments that would benefit from recoding selected legacy components using DSLs for packet filtering, data, signal, and image processing, and other latency-sensitive/security-critical functions. ***FY 2023 Plans:*** - Formulate a quantitative assessment framework for cyber risk factors, encompassing threat, consequence, and vulnerability, to enable more rigorous assessments of architectural alternatives and guide choices in software systems engineering. - Refine automated techniques for decomposing legacy code into functional modules with domain data structure and operation definitions, enabling safe replacement and enhancement of targeted components with high-level DSL code.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Integrate development environment for convergent DSL programming with decomposition tools that automate program understanding and downstream compilation tools that produce executable artifacts. - Apply tools to DoD legacy components in order to enhance security and performance while ensuring compositional correctness and safety. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects ramping up of work to develop automated techniques for decomposing legacy code into functional modules, compilation techniques for DSL virtual machine stacks, and an initial development environment.			
Title: Securing Information for Encrypted Verification and Evaluation (SIEVE)	14.500	16.000	17.500
Description: The Securing Information for Encrypted Verification and Evaluation (SIEVE) program is developing technology to enable the 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 and operationally feasible 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 2022 Plans:*** - Extend ZK proof compilers by adding problem classes as well as reducing representation size of proof statements by orders of magnitude. - Optimize post-quantum analyses to reduce theoretical proof complexity for important use cases. - Enhance techniques to permit optimization for any subset of prover computation, verifier computation, total communication, and total number of communication rounds. - Apply ZK proof techniques to additional DoD and U.S. Government use cases and evaluate their functionality, information leakage potential, and robustness to attack in collaboration with potential transition partners. ***FY 2023 Plans:*** - Extend ZK proof compilers to additional problem classes and to accommodate probabilistic problem statements. - Further enhance post-quantum analyses to reduce theoretical proof complexity for important use cases and potential transition partners. - Scale-up ZK proof techniques to realistic DoD and U.S. Government use cases and evaluate their functionality, information leakage, and robustness to attack in collaboration with potential transition partners.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Determine the feasibility of efficient, end to end verifiable, distributed architectures for private data communication that can be leveraged by overseas personnel and compatible with existing state and federal policies and regulations. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects additional effort to evaluate ZK proof techniques on realistic use cases.			
Title: Assured Micropatching (AMP) ***Description:*** The Assured Micropatching (AMP) program is developing 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, creates too much uncertainty and takes far too long to validate, 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 2022 Plans:*** - Develop a modeling capability to infer compiler optimization effects on the call graph structure, and probabilistic graph-matching and inference algorithms to produce candidate matches between the target binary procedures and most likely source code procedures. - Develop extensions to commonly used binary analysis tools to interactively show the effects of an applied micropatch. - Conduct a challenge event using a commodity controller and data logger based on a widely-used commercial data bus architecture. ***FY 2023 Plans:*** - Enable and demonstrate the automatic patching of vulnerabilities where exploitation does not involve memory corruption. - Improve and optimize the existing intermediate representations and optimize the location of the provided patch within the original binary. - Conduct a challenge event using a real-time control device in use in a cyber physical system. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects minor program repricing.	16.410	17.000	16.200
Title: Fast Network Interface Cards (FastNICs)	12.000	13.500	13.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
Description: The Fast Network Interface Cards (FastNICs) program is creating 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 memory subsystems. FastNICs aims to enable a dramatic increase in computational throughput for distributed applications such as training of machine learning systems. ***FY 2022 Plans:*** - Evaluate network interface architecture alternatives such as busses and parallelism. - Demonstrate versions of widely used distributed systems software and operating systems that accommodate massively parallel input data streams. - Demonstrate and evaluate distributed computing applications of interest to the DoD such as training deep learning systems. ***FY 2023 Plans:*** - Scale performance and demonstrate network interface hardware on multi-core central processing units (CPU's). - Evaluate versions of widely used distributed systems software and operating systems that accommodate massively parallel input data streams. - Evaluate and demonstrate machine learning applications to commercial vendors, the DoD, and IC. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects minor program repricing.			
Title: Resilient Anonymous Communication for Everyone (RACE) ***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 communication 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 statistical arguments based on realistic simulations, and not on ad hoc estimates of security. ***FY 2022 Plans:*** - Enable the system to scale to a thousand or more users by improving the efficiency of techniques for computing on encrypted routing information.	14.160	14.700	10.700

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Integrate enhanced components into the secure message-passing system with improved capability to counter a cyber adversary who has access to communication protocol information and communication nodes. - Enhance the testbed and demonstrate the integrated secure message-passing system against a simulated cyber adversary that has knowledge of the system. ***FY 2023 Plans:*** - Improve the efficiency of techniques for computing on encrypted routing information to enable the system to scale an additional order of magnitude. - Integrate enhanced components into the secure message-passing system with improved capability to counter a cyber adversary who has the capability to manipulate communication protocol information and interfere with communication nodes. - Enhance the testbed and demonstrate the integrated secure message-passing system against a simulated cyber adversary that has full knowledge of and access to the system. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects ramping down of development of obfuscation and encryption technologies, continued implementation of a secure message-passing system and testbed, and continued work to evaluate the system against a simulated cyber adversary.			
Title: Cyber-Hunting at Scale (CHASE)	16.140	15.100	7.100
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 there are few capabilities to efficiently extract and analyze the right data from the right device at the right time for DoD-scale information networks. For example, analysis of an in-memory exploit requires detailed data from a few devices, while analysis of a global botnet attack requires 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 2022 Plans:*** - Develop an analyst interface to enable automated cyber report generation, and evaluate the utility of the interface for cyber threat detection and protective measure dissemination. - Develop techniques for quantifying and reducing the risk of cyber operations. - Identify transition opportunities for validated threat detection, threat characterization, and data planning algorithms. ***FY 2023 Plans:*** - Integrate threat detection, data retention, and global analysis methods, and harden capabilities for transition to DoD stakeholders.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Transition cyber threat detection and protective measure dissemination technologies to DoD stakeholders. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease is the result of development and integration work ramping down, and the focus shifting to demonstration, hardening, and transition of cyber protection technologies to DoD stakeholders.			
Title: Memory Optimization (MemOp) ***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 2022 Plans:*** - Refine and leverage algorithm scaling for task mapping in large scale memory systems, and optimize software implementations. - Evaluate and refine integration of memory and accelerated processing pipelines. - Evaluate memory transaction implementation and develop improvements on program testbed. - Optimize algorithms and architectures for memory transaction performance in hardware and software, and evaluate on testbed. ***FY 2023 Plans:*** - Optimize integration of memory and accelerated processing pipelines and evaluate improvements on program testbed. - Harden and transition memory optimization technologies to industry and DoD. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects ramping down of development of memory optimization methods and accelerated processing pipelines, and continued use of the evaluation testbed.	18.000	17.000	8.007
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	15.320	12.400	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
varying skill levels, even those with minimal 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. ***FY 2022 Plans:*** - Scale 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, to programs of the size and complexity found in military systems. - Enhance representations of information gaps revealed by expanded cyber reasoning techniques to enable non-experts in vulnerability discovery to advance in efficacy and expertise. - Incorporate improved cyber reasoning capabilities and additional operator-requested refinements in an end-to-end, integrated computer-human software reasoning system for the DoD and IC. ***FY 2023 Plans:*** - Quantify the degree to which the cyber reasoning techniques enable non-experts in vulnerability discovery to approach expert-level efficacy. - Harden an end-to-end, integrated computer-human software reasoning system and transition to the DoD and IC. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects ramping down of work to develop and integrate technologies in a proof-of-concept, computer-human software reasoning system, and focus shifting to hardening, demonstration, and transition to the DoD and IC.			
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 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 2022 Plans:*** - Demonstrate scalability and performance of analytical capabilities on relevant large-scale data sets. - Evaluate machine-learning-based methods for identifying cyber threats across heterogeneous data, in multiple languages. - Harden cyber analytical software technologies and incorporate refinements requested by cyber operators. ***FY 2023 Plans:***	11.000	10.740	5.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Demonstrate machine-learning-based methods for identifying geographic and cultural dependencies in cyber threats and for gaining situational awareness of adversary influence operations. - Deploy software to transition partner environments. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects ramping down of efforts to implement and evaluate an integrated cyber analytical system, and focus shifting to demonstration and transition to operational partners.			
Title: Searchlight ***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 2022 Plans:*** - Improve integrated QoS management system performance in terms of scale, application identification accuracy, and application responsiveness. - Demonstrate the integrated QoS management system and evaluate its capability on heterogeneous applications distributed across wide area networks of realistic scale and complexity. - Work with transition partners to optimize the QoS management system to relevant use cases, applications, and network characteristics. ***FY 2023 Plans:*** - Demonstrate techniques for topology discovery of multiplexing sites. - Demonstrate an integrated QoS management prototype on relevant use cases and transition to DoD and commercial network service providers. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects ramping down of work to develop QoS management techniques and focus shifting to transition to the DoD and industry.	5.400	6.300	4.800
Title: Active Social Engineering Defense (ASED)	10.800	6.600	5.179

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
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 human 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 2022 Plans:*** - Demonstrate and evaluate a machine-learning-based social engineering attack detection system, including automated attribution of social engineering attacks, against advanced simulated adversaries who disguise their attacks. - Harden a modular social engineering attack detection and attribution system for use by U.S. Government, DoD, and industry. ***FY 2023 Plans:*** - Deploy social engineering attack detection software to a transition partner environment. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects a shift from development of counter-social-engineering bot technologies to technology hardening and transition to U.S. Government, DoD, and industry.			
Title: Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)	-	5.000	10.000
Description: The Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program, building on results derived in the Foundational Artificial Intelligence (AI) Science program (PE 0601101E, Project CCS-02), will develop techniques and tools to anticipate, isolate, and mitigate emergent system behaviors and thereby improve security of complex integrated software. Today's software development toolchains and testing methodologies provide very limited means for reasoning about adversarial reuse of code as written and designed. This results in unwitting creation of stable, reliable patterns of emergent behaviors within systems that adversaries can reuse in attacks. Examples include web browser exploits, which co-opt the browser's memory management algorithms and web scripts; the Spectre family of exploits; and modern bootkits, which leverage the trusted computing system management modes. In each case, attackers program emergent behaviors already present within the target system. The HARDEN approach to preventing such adversarial code reuse is to create techniques, tools, metadata, and instrumentation for reasoning about emergent execution at all stages of the software development life cycle (SDLC), and for flagging code segments and design patterns where there is high potential for adversarial reuse and emergent execution. To assess their utility, HARDEN technologies will be applied to critical system elements such as bootloaders and to integrated software systems. If successful, the technologies developed by HARDEN will facilitate efficient mitigation of complex code-			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
reuse and emergent-execution vulnerabilities at early SDLC stages, and provide the stronger roots-of-trust required by zero-trust architectures and high-assurance integrated military software systems. ***FY 2022 Plans:*** - Formulate approaches for instrumenting the development toolchain for reasoning about emergent behaviors at all available layers of abstraction, from the compiled binary code through the compiler abstractions and intermediate representations, to the highest levels of architectural abstraction. ***FY 2023 Plans:*** - Develop models and mitigations for composable emergent behaviors and for the reliable chaining of exploit primitives even where the effects of any single behavior or flaw are reduced by security mitigations. - Explore automated techniques for identifying implementations that are likely to result in composable emergent behaviors, and for suggesting transformations of implementations that, while semantically equivalent, mitigate emergent composability and thereby disrupt exploit programming. - Initiate application of concepts and techniques to critical system elements such as bootloaders and high-assurance integrated military software systems with the goal of demonstrating the capability to mitigate complex code-reuse/emergent-execution vulnerabilities at early SDLC stages. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects ramping up of work to develop techniques to mitigate emergent behaviors and initial applications of the technology to military and commercial software systems.			
Title: Signature Management using Operational Knowledge and Environments (SMOKE) ***Description:*** The Signature Management using Operational Knowledge and Environments (SMOKE) program seeks to develop signature management technologies that generate evasive cyber infrastructure by incorporating counter-attribution techniques into the design process; quantitatively measuring attribution risk in real-time; and by maintaining evasiveness after infrastructure changes in order to accelerate red team cyber operations (CO) and eliminate signatures as a source of attribution. ***FY 2023 Plans:*** - Formulate approaches for quantifying the detection and attribution risks associated with CO infrastructure development and operation. - Develop techniques for identifying patterns characteristic of CO. - Perform red team assessments of CO protection capabilities in collaboration with potential transition partners. ***FY 2022 to FY 2023 Increase/Decrease Statement:***	-	-	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
The FY 2023 increase reflects program initiation.			
Title: Hardware Optimization (HOP) ***Description:*** The Hardware Optimization (HOP) program is developing hardware optimizations for national security purposes. Specifically, HOP will enable new national security workloads in high performance microelectronic hardware. This research will produce end-to-end hardware optimization toolkits to enhance hardware designs. These toolkits will be comprised of algorithms, digital design files, documentation, and binaries. ***FY 2022 Plans:*** - Evaluate hardware optimizations to address algorithmic improvements and address scalability and performance opportunities. - Design and develop initial alternative implementations for hardware optimizations. - Provide initial hardware optimizations for performance assessments and evaluations. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.	8.000	17.100	-
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) ***Description:*** The Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) program is developing safe and reliable autonomous software agents that can neutralize botnet implants and similar large-scale malware 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 aim to enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations. ***FY 2022 Plans:*** - Enhance botnet-tracking algorithms to provide near-real-time assessment for the global identification and tracking of all major classes of botnet-conscripted networks. - Collaborate with transition partners to tailor and evaluate HACCS counter-botnet technology in realistic environments. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.	16.800	9.240	-
Title: Intent-Defined Adaptive Software (IDAS)	10.200	7.059	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
Description: The Intent-Defined Adaptive Software (IDAS) program is developing 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 2022 Plans:*** - Mature algorithmic techniques that permit verified optimization of multiple implementations, and demonstrate more efficient encoding of quality goals and operational constraints. - Demonstrate a prototype of a partially coupled implementation of a military system that has the performance of a highly-coupled, exquisitely engineered system, and the maintainability of a decoupled, modular system. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.			
Title: Configuration Security	11.400	6.050	-
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 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 2022 Plans:*** - Scale and optimize automatic generation of contextualized secure configurations for operationally relevant, complex cyber-physical-human systems, including the translation of multi-vendor, human-readable artifacts into machine-understandable formats. - Demonstrate algorithms to automatically and rapidly reconfigure a representative military operational system to a baseline that is safer, more secure, and more quickly achieved. - Demonstrate a reconfigured system that provides required functionality with automatically-generated human-readable explanations.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Transition a capability to detect and prevent malicious modification of configurations from the system-generated baseline for a shipboard communication system, and to assist system operators in changing between operational contexts. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.			
Title: Cyber Assured Systems Engineering (CASE) ***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. The challenge of resiliency is that it cannot be established through conventional testing methods. CASE is focusing 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 2022 Plans:*** - Harden technologies for cyber security systems engineering and transition to DoD stakeholders. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.	10.050	3.000	-
Title: Enhanced Attribution ***Description:*** The Enhanced Attribution program is developing technologies to associate malicious cyber actions with individual adversary 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 2022 Plans:***	8.600	3.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Harden the attribution platform and transition to operational partners. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.			
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-purpose 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 2022 Plans:*** - Harden and transition integrated network-compute capabilities to government and commercial network providers. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.	4.000	2.300	-
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS) ***Description:*** The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program developed technology to enable a black start recovery of the U.S. power grid amidst a cyber attack on the energy sector's critical infrastructure. RADICS technologies 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. The program developed 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	3.794	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
sensor spoofing. RADICS was coordinated with and transitioned technology to U.S. Government elements responsible for the defense of critical infrastructure.			
Accomplishments/Planned Programs Subtotals	240.074	237.089	183.786

	FY 2021	FY 2022
Congressional Add: AI Cyber Data Analytics (Cyber) - Congressional Add	-	15.000
FY 2022 Plans: Develop high assurance computing architectures suitable for mission-critical systems that must operate with resilience in contested environments.		
Congressional Adds Subtotals	-	15.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	151.005	203.274	193.234	-	193.234	203.757	203.184	229.627	229.537	-	-

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 also as trustworthy partners to human operators. Of particular interest are systems that can understand human language and extract information and reliably categorize content 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 and other complex software-reliant 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 2021	FY 2022	FY 2023
Title: Accelerating Artificial Intelligence (AAI)	39.000	35.100	32.000
Description: The Accelerating Artificial Intelligence (AAI) program seeks to go beyond commercially-driven advances in AI and to 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; and (2) knowledge management tools that can efficiently capture and disseminate an organization's expertise, experience and data; and (3) social context informed AI approaches to enable reliable and robust forecasting and decision aiding tools for stabilization, deterrence and gray zone operations.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
FY 2022 Plans: - Extend evaluation of novelty generators and novelty-robust AI techniques in military application domains to include new rules, goals, and events. - Demonstrate effectiveness in military applications of novelty-robust AI techniques. - Initiate transition of molecular design systems from academia and industry to DoD partners to evaluate performance in DoD applications. - Define and validate parameters for inverse design of molecules with relevance to DoD applications. - Initiate research in methods to improve human operators' ability to partner with their AI-enabled platforms in off-nominal scenarios. - Start modeling the situational awareness demands imposed by yet-to-be-built autonomous systems. - Initiate development of design tools to enable full-system human machine interface compositions. - Begin development of rapidly reconfigurable human machine interface test environments for highly automated and AI-enabled platforms. - Quantify competency-aware capabilities with relevance to DoD applications, and identify DoD experimental platforms and partners to demonstrate competency-aware capabilities. - Initiate efforts to develop a new understanding of how preconscious signals can be used to measure what people believe to be true. - Demonstrate emulated 250-milliwatt megapixel for a full format sensor with programmable in-pixel circuitry to instantiate front-end AI algorithms with outputs to back end AI processing using realistic device parameters. - Construct proof-of-concept demonstration and measure reduction in learning time increased and effectiveness of learning. - Develop means to understand concepts through grounding them in real world experiences as represented in image and video, and for automatically acquiring novel concepts representing objects and events. - Develop formal models of the structure of uncertainty in financial data sets, together with an ensemble of metrics for inconsistency among multiple data sets. - Develop techniques for identifying the specific processor likely to execute particular code segments based on control blocks identified in schematics. - Explore the use of AI and machine learning (ML) to support, and if possible automate, the generation, maintenance, and repair of proofs used in the formal verification of software. - Initiate Legal, Moral, and Ethical (LME) planning activities and develop an understanding of how escalation of force can and should be appropriately applied in the context of supervised autonomous systems. - Continue efforts to accelerate Artificial Intelligence with a focus on third wave AI.			
FY 2023 Plans: - Demonstrate competency-aware machine learning behaviors and capabilities on DoD-relevant application platforms.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Evaluate research in methods to improve human operators' ability to innovate with their AI-enabled platforms during off-nominal scenarios. - Test and refine models of the situational awareness demands imposed by yet-to-be-built autonomous systems. - Test and refine design tools to enable full-system human machine interface compositions. - Continue construction of rapidly reconfigurable human machine interface test environments for highly automated and AI-enabled platforms. - Extend efforts to measure and aggregate an individual's preconscious neural and physiological responses into actionable evidence regarding that individual's beliefs. - Develop approaches for composing identified techniques into scalable proof generation and repair capabilities within development platforms for increasing assurance of systems. - Continue LME working groups and engagements with industry and university performers to provide technical, academic, and operation expertise and advise on best practices and DoD ethical AI principles. - Continue efforts to accelerate Artificial Intelligence with a focus on third wave AI. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects a shift from development and prototyping to testing.			
Title: Symbiotic Design ***Description:*** 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 and improve the quality of deployed systems. The current generation of DoD systems and platforms integrate cyber and physical subsystems, but 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 analysis by humans and continuously-learning artificial intelligence (AI)-based co-designers. The program will create technologies essential for AI co-design: 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, quality, and innovation metrics. ***FY 2022 Plans:*** - Develop scalable design mining engines and feature extractors to enable query generation from seed designs and expand scope and domain coverage of design mining engines to allow incremental construction of design spaces.	23.040	28.100	33.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Develop approaches in machine-assisted knowledge management to establish traceable connections between software models and documentation through discovery, extraction, and linking over text, equations, tables, figures, and code. - Develop prototype tools to accelerate high fidelity model analysis and simulation, visualize and understand high dimensional design spaces, and shape and guide design exploration. - Produce design challenge problems related to sub-systems and systems of interest to the DoD, and evaluate the effectiveness of symbiotic design technologies. ***FY 2023 Plans:*** - Develop multi-domain inferencing techniques to automate multi-domain reasoning and model learning. - Scale up techniques for exploration of high-dimensional, multi-domain, combinatorial, and parametric design spaces. - Conduct design hackathons to study productivity of designers and quality of design using conventional engineering tools in comparison to when an AI co-designer and symbiotic design technologies are used. - Perform demonstration and evaluation of symbiotic design technologies through applications to sub-systems and systems of interest to the DoD. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects continued development and implementation of symbiotic design techniques and additional efforts related to demonstration and evaluation on sub-systems and systems of interest to DoD.			
Title: Knowledge-directed Artificial Intelligence Reasoning Over Schemas (KAIROS)	13.000	22.000	27.334
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 activity. 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 codify existing event-representation schemas and, when needed, create and codify 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 2022 Plans:*** - Develop capability for machine learning of the similarities and differences in the structural features of various complex event schemas. - Develop the means to curate the schema library and methods for identifying intermediate levels in the structure of the library. - Develop a user interface to probe input sources for missing information and to provide interactive feedback.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Collaborate with transition partners to evaluate systems on complex real-world event sequences and identify necessary adjustments. ***FY 2023 Plans:*** - Develop means to interpolate events of interest not reported in multiple sources that occur within complex sequences of events. - Develop means to predict future events from a sequence of complex events that is presently unfolding. - Evaluate the detection and prediction capabilities with DoD and IC users on problems related to stabilization in regional conflicts. - Optimize the system in response to operational partner assessments on complex real-world event sequences and transition the technology. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects continued development of techniques for learning complex event schemas and event discovery and prediction, and increased work to assess techniques on operational DoD and IC data.			
Title: Automated Rapid Certification Of Software (ARCOS)	27.000	25.000	24.400
Description: The Automated Rapid Certification Of Software (ARCOS) program is developing technologies that automate the capture and evaluation of software assurance evidence to enable certifiers to assess system risks earlier in the process and to commit to engineering decisions more rapidly and safely. Current software certification practices do not scale with the extent, complexity, and interconnection of software being developed by the DoD, so certification is becoming a bottleneck to new system deployment. ARCOS technologies address DoD software system certification time and cost. ARCOS technology will automatically and interactively 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 2022 Plans:*** - Develop approaches to augment assurance evidence for legacy software to provide stronger fitness arguments. - Demonstrate automatically calculated confidence measures for assurance case arguments that are objectively meaningful. - Demonstrate the composability of automatically generated assurance case arguments to support incremental evaluations. - Reduce the computation time necessary to automatically generate assurance case arguments for complex military systems. ***FY 2023 Plans:*** - Expand assurance case generation to address assurance criteria in multiple domains such as safety and security. - Develop a mechanism to track the provenance of assurance evidence used in assurance case arguments. - Demonstrate an approach to assurance-driven software development that generates evidence targeted for the high confidence software assurance required for military systems.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Demonstrate automated generation of assurance arguments for a representative complex military system. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects minor program repricing.			
Title: Learning Introspective Control (LINC)*	-	12.500	19.000
Description: *Formerly Control System Introspection The Learning Introspective Control (LINC) program will develop machine introspection and learning technologies to characterize a modified or damaged military platform from its behavior, and update the control law to maintain stability and control. The current approach to handling platform modification or damage places the burden of recovery and control on the operator, whether the operator is human or an autonomous controller. In contrast, a platform equipped with LINC technology will continually compare the real-time behavior of the platform as measured by on-board sensors with a learned model, determine if the current observed behavior of the platform differs from that model in ways that might compromise stability and control, and implement an updated control law when required. The LINC capability would aid operators in maintaining effective control of military platforms that suffer damage in battle or have been modified in the field to address emergent requirements identified during operations. ***FY 2022 Plans:*** - Develop machine introspection and learning approaches for estimating the transfer function and related control-theoretic models in real time using data from the multiple sensors organic to the platform. - Develop machine-learning based algorithms to enable the automated adaptation of a physical model representative of a system to enable it to reconstitute effective control after battle damage or in-the-field modification. - Collaborate with Service transition partners to identify high-priority military cyber-physical systems and use cases for initial experimentation. ***FY 2023 Plans:*** - Design and implement a testbed for assessing integrated machine introspection and learning approaches for operator-assisted recovery and control of military platforms that suffer damage in battle or are modified in the field. - Improve the computational efficiency of control reconstitution algorithms and expand their applicability to more complex DoD systems. - Develop a computational platform to support experiments involving cyber-physical systems and high-priority use cases in collaboration with Service transition partners. ***FY 2022 to FY 2023 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
The FY 2023 increase reflects ramping up the development of learning introspective control techniques and initiation of efforts to implement the techniques in a demonstration platform.			
Title: Counter Adversarial Artificial Intelligence ***Description:*** The Counter Adversarial Artificial Intelligence program aims to enhance the capability to detect, deflect, and diminish the effects of adversarial attacks on AI-based systems. Defense systems increasingly incorporate artificial intelligence (AI) capabilities such as machine learning and automated reasoning. These AI-enabled systems are typically engineered and optimized for environments where adversary systems are either static or strictly limited in terms of adaptive behaviors. Engagements between sophisticated AI-enabled systems are likely to become increasingly common going forward. Maintaining AI-superiority for the U.S. will require systems with higher levels of capability. Specific capabilities to be developed include recognizing when an adversary system is AI-enabled, identifying and modeling adversary AI capabilities based on empirical data, and creating counter-AI strategies including techniques to render adversary AI capabilities ineffective and/or deleterious. ***FY 2022 Plans:*** - Model the range of potential adversarial AI behaviors, including the nature of vulnerabilities in machine learning (ML) components and symbolic AI components. - Conceptualize AI systems with capabilities to detect, deflect, and diminish the effects of adversarial attacks. - Formulate approaches for recognizing when an adversary system is AI-enabled, identify and model adversary AI capabilities based on empirical data, and counter adversary AI strategies. ***FY 2023 Plans:*** - Develop and demonstrate the capability to model and learn adversarial AI behaviors and formulate approaches for using this capability to detect, deflect, and diminish the effects of adversarial attacks. - Develop techniques for establishing dimensionality reduction properties for AI-enabled systems and use these properties to constrain the extent of analysis including the number of test cases. - Develop cross-validation-based approaches for mitigating the vulnerabilities in ML-based and symbolic AI components and demonstrate the capability to render adversarial AI attacks ineffective for high-priority military use cases. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects ramping up of development of counter adversarial AI techniques and initial demonstrations of techniques on high-priority military use cases.	-	14.500	22.000
Title: Assured Autonomy ***Description:*** The Assured Autonomy program is developing rigorous design and analysis technologies for continual assurance of learning-enabled autonomous systems to enhance system safety in uncertain environments. Currently, the state of the art for test,	15.000	13.000	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
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 2022 Plans:*** - Evaluate the impact of safety-constraints incorporated in online learning algorithms on the performance of autonomous systems operating in unknown and unstructured environments. - Develop and implement improvements to formal verification tools and monitoring techniques. - Demonstrate technologies on assurance challenge problems for several learning-enabled autonomous platforms of interest to the DoD. ***FY 2023 Plans:*** - Develop integrated toolchains for end-to-end development and assurance of learning-enabled systems. - Demonstrate integrated tools on multiple autonomous systems of interest to DoD. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects the shift from development of techniques and tools to demonstrations on several learning-enabled autonomous platforms.			
Title: Active Interpretation of Disparate Alternatives (AIDA)	17.500	16.950	9.300
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, with only informal comparison among competing hypotheses. The consequence of this can be inadequate 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 2022 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Develop the means to change statistical priors for new sources to reflect known biases and reliability, and thereby enable more accurate computation of coherence measures. - Enhance interface capabilities to facilitate exploration of user-generated conjectures and other models of human-computer interaction. - Collaborate with transition partners to conduct experiments to evaluate information extraction and hypothesis generation performance on operational data. ***FY 2023 Plans:*** - Enhance the techniques for detecting important changes in otherwise similar documents to achieve a level of precision and recall necessary to enable discovery and analysis of different hypotheses. - Collaborate with transition partners to establish the utility of the technology and tailor the platform for transition partner applications. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects the shift from development of techniques for generating multiple alternative interpretations from multimedia data to evaluations of techniques on real-world data and optimization of the platform for transition partner applications.			
Title: Automating Scientific Knowledge Extraction and Modeling (ASKEM)	-	-	16.200
Description: The Automating Scientific Knowledge Extraction and Modeling (ASKEM) program will develop technologies and tools for the agile creation, sustainment, and enhancement of complex models and simulators to enable knowledge extraction and data-informed decision making in diverse scientific domains and military missions. Current modeling and simulation pipelines do not maintain the relevant inputs, assumptions, and modeling choices made during development, while rapidly changing knowledge, semantically-opaque models, and black-box simulators make pipelined development nearly impossible. ASKEM will enable a new paradigm for scientific modeling analogous to the transition in software development from the lengthy waterfall model to agile, continuous DevOps. ASKEM will produce modeling automation tools that 1) extract model components from documents and code while abstracting away from implementation details like math framework, language, and platform; 2) compose distinct model and simulator components; and 3) integrate all elements and processes in an extensible workbench that addresses the entire modeling and simulation lifecycle. ASKEM tools will enable experts to maintain, reuse, and adapt large collections of heterogeneous data, knowledge and models with traceability across knowledge sources, model assumptions, and model fitness and thereby bring agile, pipelined development to modeling and simulation. ASKEM technologies will be applied to multiple use cases to drive scalability and generality. ***FY 2023 Plans:*** - Develop formal representations and techniques for machine-assisted modeling that support automated composition and decomposition for model creation, sustainment, and customization.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Develop tools for machine-assisted simulator design and construction, enabling the rapid composition of models, frameworks, and solvers that are problem appropriate. - Develop tools for continuous machine-assisted validation of models, including construction of fitness-for-purpose simulators to accompany prognostic measures. - Initiate development of an extensible workbench that spans the entire modeling and simulation lifecycle in which the technologies can be evaluated against diverse use cases in collaboration with transition sponsors. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 increase reflects program initiation.			
Title: Artificial Intelligence Reliability and Traceability (AIRT)	-	6.000	-
Description: The Artificial Intelligence Reliability and Traceability (AIRT) program will develop design-time and run-time technologies to ensure the correct functioning of AI-enabled systems. As AI deployment scales up, it becomes more important for machine learning (ML) systems and their training data to be explainable, which means providing rationale for classifications, characterizing confidence level of the classifications, and, as a consequence, conveying an understanding of how the system will behave with similar inputs. Explainability, however, is not sufficient to ensure that ML systems meet reliability requirements and are free of bias, in the sense that the ML operates consistently with domain-focused predictive models, nor that they are traceable, in the sense that there are mappings between the models and the ML behaviors. AIRT will develop the test, evaluation, verification, and validation (TEVV) technologies that system developers need to ensure that AI-enabled systems will correctly perform their intended functions. The AIRT TEVV technologies will address the challenge of how to specify AI-related behaviors and then how to verify the specified behaviors using both analytic formal approaches, which emphasize mathematical modeling and reasoning, and traditional statistical-sampling based approaches. AIRT will also develop design principles for machine learning and related systems that enhance reliability and traceability without appreciable compromise to reasoning capability. Additionally, AIRT will develop traceability approaches that model the learning behavior of an AI component to enable developers, testers, and operators to gain detailed knowledge of how the AI system reached a computational state. The AIRT program aims to make the design and operation of AI systems more scientific and safe. ***FY 2022 Plans:*** - Formulate approaches for TEVV of AI-enabled systems and associated data to increase confidence in correct performance of intended functions. - Explore TEVV approaches that include means to specify intended AI-related behaviors and that combine analytic formal approaches, which emphasize mathematical modeling and reasoning, with traditional statistical-sampling based approaches.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
- Introduce traceability approaches akin to check-pointing and other roll-back techniques that can enhance knowledge of how an AI system reached a computational state. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.			
Title: Engineering Artificial Intelligence Systems Implementations (EAISI) ***Description:*** The Engineering Artificial Intelligence Systems Implementations (EAISI) program is creating technologies and tools to support the development of viable and trusted systems 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 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 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 techniques, tools, and practices to facilitate the development of AI-based systems that are capable, trustworthy, affordable, and timely. ***FY 2022 Plans:*** - Formulate rigorous approaches for managing training data for AI-based systems, including provenance, security, and quality, to facilitate the engineering of AI-based systems that are capable, trustworthy, affordable, and timely. - Devise approaches for testing, analyzing, and evaluating AI-based systems as means for gaining confidence in and rigorously validating those systems. - Devise a framework for integrating prototype tools in an AI systems engineering development environment for use by developers and evaluators who are not experts in AI. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.	7.300	11.800	-
Title: Explainable Artificial Intelligence (XAI) ***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	9.165	8.324	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Defense Advanced Research Projects Agency		Date: April 2022
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 2021	FY 2022	FY 2023
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 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 is developing the tools necessary to build explainable AI systems, specifically with: (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, using natural language, saliency maps, and other representations. XAI implementations will be developed and demonstrated in next-generation data analytics and autonomous systems. ***FY 2022 Plans:*** - Refine machine learning explanation systems for human-machine teaming prototypes in coordination with DoD partners. - Provide toolkit for explainable AI to DoD and IC partners targeting relevant use cases. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The FY 2023 decrease reflects program completion.			
Accomplishments/Planned Programs Subtotals	151.005	193.274	193.234

	FY 2021	FY 2022
Congressional Add: AI Cyber Data Analytics (AI) - Congressional Add	-	10.000
FY 2022 Plans: Develop scalable machine learning technologies capable of learning from large training sets with orders of magnitude less computation.		
Congressional Adds Subtotals	-	10.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A