Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Defense Advanced Research Projects Agency	Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
Total Program Element	-	463.806	383.270	333.029	-	333.029	399.233	393.917	399.742	401.742	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	27.000	11.250	15.000	-	15.000	18.750	15.000	15.000	0.000	-	-
IT-03: *CYBER SECURITY*	-	242.359	183.786	167.459	-	167.459	222.698	199.752	171.440	175.353	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	194.447	188.234	150.570	-	150.570	157.785	179.165	213.302	226.389	-	-

A. Mission Description and Budget Item Justification

The efforts described in this Program Element (PE) address the Applied Research associated with the Information and Communications Technology Program that is directed toward the application of advanced, innovative computing systems and communications technologies. This PE 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 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Defense Advanced Research Projects Agency	Date: March 2023
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*

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, 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 this 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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total
Previous President's Budget	480.363	388.270	377.426	-	377.426
Current President's Budget	463.806	383.270	333.029	-	333.029
Total Adjustments	-16.557	-5.000	-44.397	-	-44.397
• Congressional General Reductions	0.000	-5.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	-1.168	0.000			
• SBIR/STTR Transfer	-15.389	0.000			
• TotalOtherAdjustments	-	-	-44.397	-	-44.397

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2022	FY 2023
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	-

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Defense Advanced Research Projects Agency	Date: March 2023
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 2022	FY 2023
Congressional Add Subtotals for Project: IT-04	10.000	-
Congressional Add Totals for all Projects	50.000	-

Change Summary Explanation

FY 2022: Decrease reflects SBIR/STTR transfer and reprogrammings.

FY 2023: Decrease reflects a Congressional reduction for Prior Year Underexecution.

FY 2024: Decrease reflects completion of the Resilient Anonymous Communication for Everyone (RACE), Active Interpretation of Disparate Alternatives (AIDA), Memory Optimization (MemOp), Cyber-Hunting at Scale (CHASE), Computers and Humans Exploring Software Security (CHESS) and Searchlight programs in FY 2023, and a shift from development to evaluation activites in the Securing Information for Encrypted Verification and Evaluation (SIEVE) and Knowledge-directed Artificial Intelligence Reasoning Over Schemas (KAIROS) programs.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	27.000	11.250	15.000	-	15.000	18.750	15.000	15.000	0.000	-	-

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project focuses on developing the computer hardware and associated software technologies required for future computationally- and data-intensive national security applications. Powerful new approaches are needed to manage the rapid growth in available sensor data, to leverage advances in machine learning, 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 2022	FY 2023	FY 2024
Title: Underexplored Systems for Utility-Scale Quantum Computing (US2QC)	2.000	11.250	15.000
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. 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. ***FY 2023 Plans:*** - Continue evaluating 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 fault-tolerant quantum computer can succeed within a near-term timeframe.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- 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 2024 Plans:*** - Implement initial test and evaluation plans designed to verify and validate component and sub-systems required to achieve utility-scale quantum computing within a near-term timeframe. - Implement initial test and evaluation plans to verify and validate the quantum architecture underpinning a fault-tolerant quantum computer. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY2024 increase reflects a shift from initial research to test plan implementation.			
Accomplishments/Planned Programs Subtotals	2.000	11.250	15.000

	FY 2022	FY 2023
Congressional Add: Quantum Computing Acceleration - Congressional Add	25.000	-
FY 2022 Accomplishments: - Accelerated efforts to verify and validate at least one approach to fault-tolerant quantum computing. - Initiated 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. - Initiated 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 2024 Defense Advanced Research Projects Agency			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	242.359	183.786	167.459	-	167.459	222.698	199.752	171.440	175.353	-	-

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 2022	FY 2023	FY 2024
Title: Open, Programmable, Secure 5G (OPS-5G)	20.000	22.300	21.500
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 2023 Plans:*** - Develop and evaluate security architectures capable of defending Internet of Things (IoT) 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. - Demonstrate secure voice call capabilities over untrusted network nodes to commercial vendors and service providers, the DoD, and other U.S. Government stakeholders.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Test and validate integrated information protection techniques suitable for current and future mobile wireless systems to support DoD operational security needs. ***FY 2024 Plans:*** - Extend security architectures capable of defending IoT-class devices while minimizing power requirements. - Incorporate formally verified code in programmable switches to augment the security of network defenses. - Develop an operationally relevant network stack and demonstrate secure 5G core networking at DoD installations for multiple use cases. - Deploy technologies in commercially available user equipment and a U.S. mobile network operator. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects the shift from development and implementation of 5G network security technologies to demonstration and evaluation of these technologies in collaboration with industry, DoD, and U.S. Government stakeholders.			
Title: Program Analysis for Capability Excellence (PACE) ***Description:*** The Program Analysis for Capability Excellence (PACE) program is developing tools and techniques to autonomously identify adversary compromise of software, mitigate negative effects of adversary capabilities, and restore the integrity of compromised software. PACE enables rapid, autonomous response to cyber attacks without using source code or requiring recompilation. ***FY 2023 Plans:*** - Develop a prototype autonomous system to identify and mitigate software compromise for a range of systems of increasing complexity. - Demonstrate and evaluate the capabilities of the prototype autonomous 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 2024 Plans:*** - Demonstrate the versatility of the system by increasing the complexity of the 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. - Collaborate with transition partners to improve and further develop systems to identify and mitigate software compromise that align with user needs. ***FY 2023 to FY 2024 Increase/Decrease Statement:***	16.000	22.000	17.360

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 decrease reflects the shift from development of techniques for autonomously identifying and mitigating compromise to demonstration and assessment of these techniques.			
Title: Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)	14.750	18.000	18.000
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 incremental software (re)engineering the benefits of formal software verification currently available only to clean-slate development efforts. ***FY 2023 Plans:*** - 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. - Integrate development environment for convergent DSL programming with decomposition tools that automate program understanding and downstream compilation tools that produce executable artifacts. - Demonstrate utility by replacing a component in a large legacy distributed system. - Apply tools to DoD legacy components in order to enhance security and performance while ensuring compositional correctness and safety. ***FY 2024 Plans:*** - Extend user interface to enable inference of specifications most relevant to component domains and most useful for verification goals. - Develop additional analysis and synthesis passes to increase the percentage of legacy code that can be enhanced by the tools. - Develop connections between component interface models and architectural modeling tools to facilitate adoption by developers. - Demonstrate the enhancement of software components for a platform representative of DoD needs.			
Title: Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)	5.000	11.000	15.500

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
Description: The Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program is developing 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. The HARDEN approach to preventing 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-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 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 2024 Plans:*** - Refine tools involving formal methods and hardware inference engines for reasoning about emergent behaviors and mitigating against exploit programming to scale from component-level analysis to subsystems. - Formalize description languages to construct models of emergent execution including operational exploits and to facilitate usage by non-formal modeling experts. - Establish an initial Development, Security, and Operations (DevSecOps)-enabled infrastructure and associated workflow to enable integration and facilitate flow from modeling to tooling. - Perform initial evaluation of the effectiveness and accuracy of tools, employing methods such as white-box testing and reverse engineering. ***FY 2023 to FY 2024 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 increase reflects expanded development of techniques to mitigate emergent behaviors and initiation of efforts to evaluate the effectiveness of the tools in mitigating code-reuse and emergent-execution vulnerabilities.			
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 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 demonstrating patching of a real-time control device currently in use in a cyber physical system. ***FY 2024 Plans:*** - Update micropatch positioning and verifiability adjustments for challenge platforms and patch types. - Demonstrate the automatic patching of vulnerabilities for additional use cases of interest to the DoD. - Conduct a challenge event of a networked system of electronic control modules interoperating over a standard data bus used in commercial vehicles, with appropriate test cases for the whole-system evaluation. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects the shift from development of technologies to enable the rapid production of targeted micropatches to demonstration of these tools and techniques on systems of interest to the DoD.	17.000	16.200	9.000
Title: Securing Information for Encrypted Verification and Evaluation (SIEVE) ***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	16.000	17.500	9.500

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
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 2023 Plans:*** - Determine the feasibility of efficient, end to end verifiable, distributed architectures for private data communication. - 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. ***FY 2024 Plans:*** - Develop and demonstrate technologies to enhance the privacy of users of cloud, internet, and wireless technologies to enhance DoD operational security and counter digital authoritarianism. - Formulate high-fidelity emulators and modeling tools to enable integration of quantum communications with classical networks. - Optimize ZK proof techniques and quantify the functionality, information leakage, and robustness to attack of ZK proof technology in collaboration with potential transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects ramping down of work to develop ZK proof techniques and focus shifting to evaluation on realistic use cases of interest to the DoD.			
Title: Fast Network Interface Cards (FastNICs)	11.000	12.000	5.999
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 2023 Plans:*** - Scale performance and demonstrate network interface hardware on multi-core central processing units.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Design and develop high-fidelity network simulation to enable accurate performance modeling of workflows over various network topologies. - Evaluate versions of widely used distributed systems software and operating systems that accommodate massively parallel input data streams, and demonstrate machine learning applications to commercial vendors, the DoD, and Intelligence Community. ***FY 2024 Plans:*** - Extend machine learning algorithms to increase hardware utilization and reduce power consumption. - Demonstrate accurate performance modeling of workflows over various network topologies using high-fidelity network simulation capability. - Augment machine learning applications to operate over DoD and commercially available network topologies. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects the shift from development of advanced input/output technologies to workflow demonstrations on DoD and commercial networks.			
Title: Signature Management using Operational Knowledge and Environments (SMOKE)	-	15.179	22.000
Description: The Signature Management using Operational Knowledge and Environments (SMOKE) program will develop signature management technologies that generate evasive cyber infrastructure which minimizes signatures as a source of attribution. SMOKE will accomplish this goal by incorporating counter-attribution techniques into the design process; quantitatively measuring attribution risk in real-time; and maintaining evasiveness after infrastructure changes. SMOKE will develop data-driven tools to automate the planning and execution of threat emulated cyber infrastructure needed for network security assessments by red teams. SMOKE will also develop data-driven tools to automate the discovery of cyber threat infrastructure signatures. SMOKE will prototype components that enable red teams to plan, build, and deploy cyber infrastructure that is informed by machine-readable signatures of sophisticated cyber threats. ***FY 2023 Plans:*** - Formulate concepts for signature management technologies that enable evasive cyber infrastructure. - Develop tools to automate the acquisition, management, and disposal of red team cyber infrastructure that mimics advanced cyber threat actors, to extract infrastructure associations from large-scale cyber datasets, and to generate machine readable signatures of advanced cyber threats. - Initiate design and implementation of a distributed development environment that enables concurrent development and operational assessment across the military services and commands as a means for accelerating the creation of new cyber capabilities. ***FY 2024 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Extend cyber planning and generation tools to recommend and execute red team cyber operations plans with contingencies based on real-time attribution risk assessments. - Develop techniques for collecting red team cyber infrastructure emissions and generating attribution risk assessments. - Evaluate red team cyber operations planning and generation capabilities in collaboration with potential transition partners. - Perform integrated demonstrations and initial evaluations of red team capabilities in collaboration with potential transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects scaling up of efforts to develop signature management technologies and initiation of performance evaluations in collaboration with potential transition partners.			
Title: Cyber Agents for Security Testing and Learning Environments (CASTLE) ***Description:*** The Cyber Agents for Security Testing and Learning Environments (CASTLE) program, expanding on approaches initiated in the Cyber-Hunting at Scale (CHASE) program (PE 0602303E, Project IT-03), will develop an AI-toolkit to instantiate realistic network environments and train cyber agents to enable resilient network operations against advanced persistent threats (APTs). CASTLE will formulate network hardening as a reinforcement learning (RL) problem and teach RL agents to operate through the post-breach behavior of widely available penetration testing tools. Over progressive rounds of attack and defense, agents will explore defensive actions to proactively stop on-going attacks while maintaining operationally relevant workflows. Environments will execute agents inside instrumented subnets that are deployed to live networks and will simulate defensive actions that counter APT tools. Agent execution will produce calibrated datasets for progressively improving simulations. The defensive cyber agents developed under CASTLE will provide the DoD with continual security assessments of critical networks and real-time response to cyber attacks. ***FY 2023 Plans:*** - Formulate intelligent cyber agents that learn to identify attacker tools from calibrated datasets and training in realistic network environments. - Develop workflow definitions and selection criteria for assessing reinforcement learning based defensive cyber agents. ***FY 2024 Plans:*** - Develop approaches for intelligent cyber agents to devise defensive measures against cyber attacks. - Develop defensive and assessment actions and application programming interface for agent execution. - Develop simulation and execution environment for evaluating cyber agent decision-making and performance. - Develop a library of APT test cases for cyber agent learning rates, effectiveness, and overhead in realistic DoD network environments. ***FY 2023 to FY 2024 Increase/Decrease Statement:***	-	8.000	16.000

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 increase reflects program scaling up to develop reinforcement learning based defensive cyber agents and the simulation and execution environment for performance evaluation.			
Title: Constellation	-	10.000	20.000
Description: The Constellation program, building upon all cyber security technologies developed in this PE and Project, will develop technologies, capabilities, and prototype systems to enable full spectrum military cyberspace operations to deter, disrupt, and if necessary, defeat adversary cyber actors to defend the U.S. Constellation is a collaborative effort involving the cyber operator, acquisition, and developer communities, who will collectively prioritize, select, plan, and approve the development and demonstration of operational prototype systems based on the results of completed and on-going basic and applied research efforts. In this way, Constellation will provide a bridge between S&T and acquisition. Once a specific operational prototype has been selected and approved for development under Constellation, agile development, security, and operations (DevSecOps) will be used to enable operator feedback to drive development and thereby ensure relevance to highly dynamic cyber missions. Technologies of interest include but are not limited to artificial intelligence (AI), machine learning (ML), and data science (DS); resilient software, networking, and computing systems; data and information assurance; and cyber threat intelligence. The work achieves high relevance through close coordination with U.S. cyber operators and the use as appropriate DevSecOps and other collaborative development processes. The work achieves high velocity through streamlined acquisition, assessment, approval, and deployment processes. The Constellation program is funded from both PE 0602303E, Project IT-03 and PE 0603760E, Project CCC-05 to facilitate rapid transition of cyber technologies, capabilities, and prototype systems to programs of record and operations. Of particular interest are technologies developed under the Cyber Hunting at Scale (CHASE), Harnessing Autonomy for Countering Cyber adversary Systems (HACCS), and Program Analysis for Capability Excellence (PACE) programs and under development in the Cyber Agents for Security Testing and Learning Environments (CASTLE), and Signature Management using Operational Knowledge and Environments (SMOKE) programs. Constellation represents a new paradigm for the rapid and continuous delivery of cyber technologies, capabilities, and prototype systems into operational use for the DoD. ***FY 2023 Plans:*** - Formulate collaborative processes for prioritization, selection, planning, and approval of efforts to develop technologies, capabilities, and prototype systems to enable full spectrum military cyberspace operations. - Collaborate across operator, acquisition, and developer communities to initiate efforts to create operational prototypes for selected high-priority cyber missions. ***FY 2024 Plans:*** - Coordinate with operators from Commands and Services to formulate current cyber operations challenges as problems for which AI/ML/DS-based approaches hold promise.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Coordinate with developers and systems administrators to develop and implement the advanced infrastructure needed for real-time AI/ML/DS-enabled cyber operations, including the large-scale cyber data and high-performance computing necessary for training and assessment of adaptive and learning algorithms. - Coordinate with systems owners to understand the advantages and disadvantages of architectural alternatives to facilitate accelerated transition to cyber programs of record. - Coordinate with cyber acquisition offices to initiate pipelined development of cyber operational prototypes through the use as appropriate of development, security, and operations (DevSecOps) and other collaborative development processes and of streamlined acquisition, assessment, approval, and deployment processes. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects the expansion of efforts to transition results arising from cyber programs in this PE and Project.			
Title: Securing the Software Supply Chain ***Description:*** The Securing the Software Supply Chain program will create software development technologies that provide visibility into the software components incorporated and the build chain employed in the creation of complex programs that reuse open and other diverse sources. Software supply chain attacks (e.g., SolarWinds) are growing in sophistication and severity. These attacks are enabled by the long complex chains of software reuse which hide dependencies and increase the difficulty of finding and remediating vulnerabilities. The growing dependence on open-source software, where contributor motives may also be obscure, further exacerbates this problem. In addition, lack of knowledge regarding the build chain by which source code is compiled, linked, and loaded results in an executable program about which very little is known, and so the problem of opacity is reinforced at multiple stages in the software development process. The program will develop technologies for automatically tracking the software bill of materials (SBOM), including for software with uncertain provenance, as an important step towards mitigating software supply chain risks. ***FY 2024 Plans:*** - Create methods that identify explicit and implicit software dependencies based on automated program and development environment understanding. - Develop automated techniques for collecting or inferring detailed information about the build chain used to create the executable from the source code. - Develop techniques for identifying and tracking high-risk open-source activities. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects program initiation.	-	-	6.600
Title: Automated Assessment of Vulnerabilities (AAV)	-	-	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
Description: The Automated Assessment of Vulnerabilities (AAV) program will create technology to automatically and accurately assess the vulnerability of software systems with state-of-the-art defenses. At present, techniques to measure the severity of software vulnerabilities focus on the exploitability of individual vulnerabilities and ignore the possibility of sequencing exploits into chains, thereby magnifying their severity. To obtain a more accurate assessment, AAV will map vulnerabilities back to the underlying flaw, identify its pre- and post-conditions, and use program analysis and machine learning to assess the potential for composing the associated exploits. ***FY 2024 Plans:*** - Formulate approaches for mapping the symptoms of a vulnerability back to the underlying flaw and for identifying pre- and post-conditions. - Develop techniques to accurately assess the severity of a vulnerability chain in software systems with state-of-the-art defenses. - Develop approaches to identify and mitigate vulnerabilities in business process applications. - Explore and prioritize demonstrations of severity analysis on vulnerabilities of interest to transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects program initiation.			
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 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 knowledge of and access to the system. ***FY 2023 to FY 2024 Increase/Decrease Statement:***	14.700	8.700	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 decrease reflects program completion.			
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 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 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects program completion.	17.000	7.007	-
Title: Cyber-Hunting at Scale (CHASE) ***Description:*** The Cyber-Hunting at Scale (CHASE) program is developing data-driven tools for real-time cyber threat detection, characterization, and protection within enterprise-scale networks. U.S. computer networks are continually under attack, but at present 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 2023 Plans:*** - Integrate threat detection, data retention, and global analysis methods, and harden capabilities for transition to DoD stakeholders. - Transition cyber threat detection and protective measure dissemination technologies to DoD stakeholders. ***FY 2023 to FY 2024 Increase/Decrease Statement:***	15.100	6.100	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 decrease reflects program completion.			
Title: Computers and Humans Exploring Software Security (CHESS)	12.400	5.000	-
Description: The Computers and Humans Exploring Software Security (CHESS) program is developing technologies to enable computers and humans to reason collaboratively over software artifacts, such as source code and compiled binaries, with the goal of finding vulnerabilities more rapidly and accurately than unaided human operators. CHESS envisions a future in which high-intensity cyber operations are conducted by computer-human teams. CHESS capabilities will be designed for use by humans of varying skill levels, even those with 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 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 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects program completion.			
Title: Searchlight	6.300	4.800	-
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 2023 Plans:*** - Demonstrate an integrated QoS management prototype on relevant use cases and transition to DoD and commercial network service providers. ***FY 2023 to FY 2024 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 decrease reflects program completion.			
Title: Active Social Engineering Defense (ASED) ***Description:*** The Active Social Engineering Defense (ASED) program developed 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 prevented 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 greatly reduced the effectiveness of adversary social engineering attacks and improve the security of DoD information systems.	6.600	-	-
Title: Cora ***Description:*** The Cora program developed 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 assisted cyber analysts by providing them with pre-processed cyber leads that otherwise might not be available.	10.740	-	-
Title: Hardware Optimization (HOP) ***Description:*** The Hardware Optimization (HOP) program developed hardware optimizations for national security purposes. Specifically, HOP enabled new national security workloads in high performance microelectronic hardware. This research produced end-to-end hardware optimization toolkits to enhance hardware designs. These toolkits are comprised of algorithms, digital design files, documentation, and binaries.	17.100	-	-
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) ***Description:*** The Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) program developed safe and reliable autonomous software agents that can neutralize botnet implants and similar large-scale malware in networked devices. HACCS developed 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	9.240	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
effects to systems and infrastructure. HACCS technologies enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations.			
Title: Intent-Defined Adaptive Software (IDAS) ***Description:*** The Intent-Defined Adaptive Software (IDAS) program developed 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 developed techniques for deferring software concretizations until uncertainties are resolved, either at build time or during run time, for complex systems. IDAS technology can significantly reduce software development time and maintenance costs, thereby enabling DoD to acquire, sustain, and improve software-based capabilities more cost-effectively.	6.379	-	-
Title: Configuration Security ***Description:*** The Configuration Security program developed 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 developed capabilities to automate the appropriate configuration of such systems within the operational context, ensure secure configuration settings, and prevent malicious changes to these settings.	6.050	-	-
Title: Cyber Assured Systems Engineering (CASE) ***Description:*** The Cyber Assured Systems Engineering (CASE) program developed 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 formulated 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 focused 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	3.000	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
networked cyber-physical systems. CASE technologies enable the design of cyber-physical systems that robustly execute their intended function despite the efforts of sophisticated cyber adversaries.			
Title: Enhanced Attribution ***Description:*** The Enhanced Attribution program developed technologies to associate malicious cyber actions with individual adversary operators, and to publicly reveal these actions without compromising sources and methods. The program focused 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 were developed and showed promise, they provided the basis for new cyber capabilities such as indications and warning of adversary cyber actions. These technologies were implemented in tools for evaluation by potential transition partners.	3.000	-	-
Accomplishments/Planned Programs Subtotals	227.359	183.786	167.459

	FY 2022	FY 2023
Congressional Add: AI Cyber Data Analytics (Cyber) - Congressional Add	15.000	-
FY 2022 Accomplishments: - Formulated translation layers between currently siloed binary analysis tools to accelerate progress and enhance capabilities across binary analysis stacks. - Formulated development-to-deployment remote attestation capabilities that can be verified and deployed on a DoD-relevant Zero-Trust Architecture application. - Explored prototype systems that provide confidentiality, integrity, and availability of messaging to enable privacy of communication even in hostile settings. - Extended location-aware privacy capabilities to enhance the operational security of DoD and U.S. Government personnel outside of the continental U.S. - Enhanced technologies and integrated in a simulation platform to facilitate evaluation of power grid restoration capabilities.		
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 2024 Defense Advanced Research Projects Agency			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	194.447	188.234	150.570	-	150.570	157.785	179.165	213.302	226.389	-	-

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, 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 this 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 2022	FY 2023	FY 2024
Title: Accelerating Artificial Intelligence (AAI)	55.000	47.500	30.365
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 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
FY 2023 Plans: - Evaluate research in methods to improve human operators' ability to innovate with their AI-enabled platforms during off-nominal scenarios including simulated system failures. - Develop, test, and refine models of the situational awareness demands imposed by yet-to-be-built autonomous systems. - Develop, test, and refine design tools for composing whole-system human machine interfaces. - 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. - Formulate preliminary methods for converting interview questions into stimuli that evoke preconscious neural and physiological responses. - Identify variables that confound the data collection process necessary for aggregating an individual's preconscious response to stimuli. - Demonstrate improved computational efficiency of scalable methods to generate accurate statistics at the outputs of machine learning systems, enabling improved sensor fusion. - Refine approaches for composing techniques into scalable proof generation and repair capabilities within development platforms to increase assurance of systems. - Conduct Legal, Moral, and Ethical (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. - Develop foundational AI science, advance the state of the art in AI engineering, and create human-machine teaming approaches that support trustworthy AI for mission- and safety-critical domains.			
FY 2024 Plans: - Develop and evaluate methods to improve human operators' ability to innovate with their AI-enabled platforms during off-nominal scenarios including unanticipated contexts. - Test and refine models of the situational awareness demands imposed by yet-to-be-built autonomous systems. - Test and refine design tools for composing whole-system human machine interfaces. - Refine and mature a rapidly reconfigurable human machine interface test environment for highly automated and AI-enabled platforms. - Refine methods for converting interview questions into stimuli that evoke preconscious neural and physiological responses. - Mitigate variables that confound the data collection process necessary for aggregating an individual's preconscious response to stimuli.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Continue to develop foundational AI science, advance the state of the art in AI engineering, and create human-machine teaming approaches that support trustworthy AI for mission- and safety-critical domains. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects a shift from development and prototyping to testing.			
Title: Learning Introspective Control (LINC)	12.500	19.000	23.000
Description: The Learning Introspective Control (LINC) program is developing 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 would 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 2023 Plans:*** - Develop control reconstitution algorithms with performance and computational efficiency necessary for complex DoD systems. - Design and implement a testbed for assessing integrated machine introspection and learning approaches for automated recovery and control of military platforms that suffer damage in battle or are modified in the field. - Develop a computational platform to support experiments involving cyber-physical systems and high-priority use cases in collaboration with Service transition partners. ***FY 2024 Plans:*** - Demonstrate computational efficiency of control reconstitution algorithms and establish suitability for integration in DoD systems that have limited spare computational resources. - Integrate initial machine introspection and learning algorithms on the testbed and make performance measurements to establish the feasibility of automated recovery and control of military platforms that suffer damage in battle or are modified in the field. - Perform experiments involving recovery and control of cyber-physical systems and high-priority use cases in collaboration with Service transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 increase reflects ramping up the development of learning introspective control techniques and implementation in a demonstration platform, and initiation of experiments in collaboration with Service transition partners.			
Title: Symbiotic Design	28.100	24.500	22.500
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 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 2024 Plans:*** - Develop new mathematical techniques to address topological and 3D placement challenges in complex cyber physical systems design. - Develop integrated toolchains that construct design spaces for a given (partial or complete) design problem and seed designs; automatically compose and evaluate a design point; and explore high-dimensional, multi-domain combinatorial design spaces. - Conduct design hackathons to study the performance and originality of the cyber-physical systems designed using the integrated symbiotic design technologies and toolchains. - Demonstrate and evaluate symbiotic design technologies and integrated toolchains for complex systems of interest to the DoD. ***FY 2023 to FY 2024 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 decrease reflects ramping down of development and implementation of symbiotic design techniques and focus shifting to evaluation of technologies and integrated toolchains on complex systems of interest to the DoD.			
Title: Knowledge-directed Artificial Intelligence Reasoning Over Schemas (KAIROS)	22.000	25.300	13.000
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 multimedia 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 2023 Plans:*** - Develop the means to interpolate events of interest not reported in multiple sources that occur within complex sequences of events. - Develop the means to predict future events from a sequence of complex events as it is unfolding. - Evaluate the event detection and prediction capabilities with DoD and Intelligence Community (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 initiate transition of the technology. ***FY 2024 Plans:*** - Develop the means to compute and display sequential information about the constituent events in a complex event and specify when order is or is not important in the sequence. - Design and run an evaluation with potential users to determine the effectiveness of the event schema-based platform in comparison with existing tools. - Prepare an end-to-end analytic platform as well as a schema creation platform for transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects ramping down of development of techniques for learning complex event schemas and event discovery and prediction, and focus shifting to evaluation of techniques and refinements to facilitate transition.			
Title: Automated Rapid Certification Of Software (ARCOS)	25.000	22.000	12.000

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
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 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 appropriate for the high confidence software assurance required for military systems. - Demonstrate automated generation of assurance arguments for a representative complex military system. ***FY 2024 Plans:*** - Demonstrate automated assurance case generation and composition to enable simultaneous evaluation of assurance criteria in multiple domains such as safety and security. - Demonstrate assurance-driven software development for a representative complex military system that requires high confidence software assurance. - Integrate and harden technologies for automated generation of assurance arguments for use by potential transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects ramping down of development of assurance generation techniques and focus shifting to demonstration, hardening, and transition of the software assurance technology.			
Title: Assured Autonomy	13.000	9.400	5.005
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, 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			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
the DoD to more rapidly and efficiently deploy learning-enabled autonomous systems that can be trusted to operate safely in uncertain environments. ***FY 2023 Plans:*** - Develop integrated toolchains for end-to-end development and assurance of learning-enabled systems. - Develop a framework for continuous assurance and provenance of evidentiary artifacts. - Demonstrate integrated tools on multiple autonomous systems of interest to DoD. ***FY 2024 Plans:*** - Transition integrated toolchain and assurance tools to DoD partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects a shift from assurance toolchain integration and demonstration to transition of an integrated toolchain to DoD partners.			
Title: Automating Scientific Knowledge Extraction and Modeling (ASKEM) ***Description:*** The Automating Scientific Knowledge Extraction and Modeling (ASKEM) program is developing 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 enables a new paradigm for scientific modeling analogous to the transition in software development from the lengthy waterfall model to agile, continual Development and Operations (DevOps). ASKEM modeling automation tools 1) extract model components from documents and code while abstracting 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 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. - Develop tools for machine-assisted simulator design and construction to enable the rapid composition of models, frameworks, and solvers that are problem appropriate.	-	19.200	23.700

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Develop tools for continual machine-assisted validation of models, including construction of fitness-for-purpose simulators. - Initiate development of an extensible workbench that spans the entire modeling and simulation lifecycle to facilitate technology evaluation on diverse use cases in collaboration with transition partners. ***FY 2024 Plans:*** - Establish baselines and measure technical component performance for accuracy, timeliness, maintainability, and scalability in selected evaluation domains. - Implement and test all interfaces and components, develop initial human-machine interface, integrate workbench prototype, and validate technical component integration on papers-to-prediction tasks. - Evaluate utility of the integrated system by comparing performance of modelers working with and without the tools on multiple tasks. - Demonstrate and initiate evaluation of the workbench across the entire modeling and simulation lifecycle against diverse use cases in collaboration with transition partners. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects continued development of model construction and assembly technologies and scaling up of implementation of technologies in an integrated workbench and evaluation in collaboration with transition partners.			
Title: Assured Neuro Symbolic Learning and Reasoning (ANSR)	-	11.000	14.000
Description: The Assured Neuro Symbolic Learning and Reasoning (ANSR) program, building on results derived in the Engineering Artificial Intelligence Systems Implementations (EAISI) program (PE 0602303E, Project IT-04), develops new hybrid AI algorithms that deeply integrate symbolic reasoning with data driven learning to create trustworthy AI-based systems. Here, an AI based system is considered trustworthy if it is: (a) robust to domain informed and adversarial perturbations, (b) supported by an assurance framework that creates and analyzes heterogenous evidence towards safety and risk assessments, and (c) predictable with respect to some specification and model of fitness. ANSR develops hybrid AI algorithms for which it is possible to develop evidence-based techniques that support confident assurance judgments. The key idea is to interleave symbolic and neural representations in hybrid AI algorithms that are capable of acquiring symbolic knowledge through learning and performing symbolic reasoning at scale to deliver robust inference, generalize to new situations, and provide evidence for assurance and trust. ANSR technologies will be demonstrated and evaluated on DoD use cases such as autonomy where trustworthiness is essential. ***FY 2023 Plans:*** - Formulate approaches to extract symbolic knowledge from neural network representations. - Initiate development of a pipeline that abstracts neuro symbolic algorithms into formally analyzable representations and evaluates them with respect to a set of mission dependent specifications.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
- Develop initial use cases and an architecture for engineering and demonstrating mission relevant applications of hybrid AI algorithms. ***FY 2024 Plans:*** - Develop and model new hybrid AI algorithms and architectures that deeply integrate symbolic reasoning with data driven machine learning. - Develop an assurance framework and methods for deriving and integrating evidence of correctness and adversarial scenarios for assessing the robustness of hybrid AI algorithms. - Perform initial demonstration and evaluation of hybrid AI technologies and their composition in systems through use cases of interest to the DoD. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 increase reflects ramping up of development of techniques that integrate symbolic reasoning with data-driven machine learning and initiation of evaluation on high priority use cases of interest to the DoD.			
Title: Learning Autonomy in Synthetic Environments (LASE)	-	-	7.000
Description: The Learning Autonomy in Synthetic Environments (LASE) program will develop simulation-to-simulation and simulation-to-real neuro-symbolic transfer learning techniques that enable more fully unmanned operations by autonomous systems. The autonomy levels of unmanned systems of today are limited because it is assumed that the modeling and simulation (M&S) training environment captures all the relevant phenomena at a high fidelity, when in reality it does not account for the data domain shift common when translating simulation outcomes from the M&S environment to the real world. The LASE approach will integrate symbolic structures (to capture discrete symbolic phenomena like mission objectives) and neural structures (to generalize and encode high-dimensional phenomena like sensor signals, imagery, etc.) to more realistically transfer learned autonomy from a M&S environment. Furthermore, since it is often difficult to choose an appropriate M&S training environment, LASE will also explore the development of a neuro-symbolic digital twin for use in training. LASE transfer of M&S-based learning will enable higher levels of autonomy for systems that operate in environments where command, control, and communications can be restricted or denied. ***FY 2024 Plans:*** - Identify universal features of neural perception and symbolic reasoning for sequential decision-making tasks in reinforcement learning. - Formulate approaches for integrating symbolic and neural structures for autonomous systems with higher levels of autonomy. - Develop use cases and a testbed for evaluating performance in terms of time-to-threshold and long-run performance of the neuro-symbolic transfer learning solutions when compared to other transfer learning baselines. ***FY 2023 to FY 2024 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
The FY 2024 increase reflects program initiation.			
Title: Active Interpretation of Disparate Alternatives (AIDA) ***Description:*** The Active Interpretation of Disparate Alternatives (AIDA) program is developing a multi-hypothesis semantic engine that generates alternative interpretations of events, situations, and trends from a variety of unstructured sources 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 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 2023 to FY 2024 Increase/Decrease Statement:*** The FY 2024 decrease reflects program completion.	12.800	10.334	-
Title: Counter Adversarial Artificial Intelligence ***Description:*** The Counter Adversarial Artificial Intelligence program enhanced 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 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.	6.000	-	-
Title: Engineering Artificial Intelligence Systems Implementations (EAISI) ***Description:*** The Engineering Artificial Intelligence Systems Implementations (EAISI) program created technologies to support the development of assured systems that include AI and machine learning (ML) capabilities. Modern AI-dependent systems may	5.047	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
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 2022	FY 2023	FY 2024
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 developed hybrid, neuro symbolic architectures that facilitate the analysis and synthesis of complex systems that must rely on AI-based components.			
Title: Explainable Artificial Intelligence (XAI) ***Description:*** The Explainable Artificial Intelligence (XAI) program developed a new generation of machine learning techniques that are able to explain their rationale, characterize their strengths and weaknesses, and convey an understanding of how they will behave in the future. AI is a critical enabler for U.S. military systems that will perform increasingly complex and sensitive missions. However, in order for developers, users, and senior leaders to feel confident enough to deploy and use AI-enabled systems, these systems must be able to explain their rationale, and their recommendations, decisions, and actions must be delivered in a way that military users can understand and trust. Today, most machine learning systems provide no explanations, or provide explanations that are 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 developed 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 were developed and demonstrated in next-generation data analytics and autonomous systems.	5.000	-	-
Accomplishments/Planned Programs Subtotals	184.447	188.234	150.570

	FY 2022	FY 2023
Congressional Add: AI Cyber Data Analytics (AI) - Congressional Add	10.000	-
FY 2022 Accomplishments: - Developed techniques to extract knowledge from structured data as part of an end-to-end automated knowledge extraction and modeling process. - Developed techniques for tracking the provenance of evidentiary artifacts to support model-based engineering and continuous assurance of high-confidence software systems. - Developed evidence curation tools to enable secure software systems engineering and evidence-based assurance judgments. - Augmented AI-based design tools to enhance applicability to unmanned underwater vehicles and air mobility vehicles.		

Exhibit R-2A, RDT&E Project Justification: PB 2024 Defense Advanced Research Projects Agency		Date: March 2023
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-04 / *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*

	FY 2022	FY 2023
- Enhanced user interfaces to facilitate event schema curation and provide feedback for event schema recognition systems.		
Congressional Adds Subtotals	10.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A