Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Defense Advanced Research Projects Agency	Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
Total Program Element	-	365.033	333.029	397.266	-	397.266	453.711	510.600	539.845	559.063	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	12.770	15.000	46.805	-	46.805	53.455	60.158	63.603	65.868	-	-
IT-03: *CYBER SECURITY*	-	220.380	167.459	185.714	-	185.714	212.101	238.695	252.367	261.351	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	131.883	150.570	164.747	-	164.747	188.155	211.747	223.875	231.844	-	-

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, cyber-physical and embedded systems, critical infrastructure, and other computation-intensive mission-critical 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 2025 Defense Advanced Research Projects Agency	Date: March 2024
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*

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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	383.270	333.029	399.233	-	399.233
Current President's Budget	365.033	333.029	397.266	-	397.266
Total Adjustments	-18.237	0.000	-1.967	-	-1.967
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	-4.968	0.000			
• SBIR/STTR Transfer	-13.269	0.000			
• TotalOtherAdjustments	-	-	-1.967	-	-1.967

Change Summary Explanation

FY 2023: Decrease reflects SBIR/STTR transfer and reprogrammings.
FY 2024: N/A
FY 2025: Decrease reflects minor program repricing.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency			Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	12.770	15.000	46.805	-	46.805	53.455	60.158	63.603	65.868	-	-

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 2023	FY 2024	FY 2025
Title: Underexplored Systems for Utility-Scale Quantum Computing (US2QC)	12.770	15.000	46.805
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 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Explore strategies for expanding the number of underexplored approaches to fault tolerant quantum computing that can be effectively evaluated by this effort. ***FY 2025 Plans:*** - Begin experimental verification and validation of components and sub-systems required to achieve utility-scale quantum computers within a near-term timeframe. - Begin evaluation of a scalable and fabricable design for a fault-tolerant prototype of a utility-scale quantum computer. - Develop key system performance metrics for prototype designs and initial specification targets for all components and subsystems. - Identify and procure long-lead hardware items needed to perform prototype research and development. - Evaluate an additional system engineering point design for building a fault-tolerant quantum computer. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects a shift from initial test plan implementation to full system evaluation.			
Accomplishments/Planned Programs Subtotals	12.770	15.000	46.805

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency			Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	220.380	167.459	185.714	-	185.714	212.101	238.695	252.367	261.351	-	-

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, cyber-physical and embedded systems, critical infrastructure, and other computation-intensive mission-critical 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 2023	FY 2024	FY 2025
Title: Constellation	31.418	28.000	43.000
Description: The Constellation program is developing technologies, capabilities, and prototype systems to enable full spectrum military cyberspace operations to deter, disrupt, and defeat adversary cyber actors and to defend the U.S. 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 of development, security, and operations (DevSecOps) and other collaborative development processes. The work achieves high velocity through streamlined acquisition, assessment, approval, and deployment processes. Constellation development and deployment pipelines enable the rapid and continuous delivery of cyber technologies, capabilities, and prototype systems into operational use for the DoD. The Constellation program is funded in PE 0602303E, Project IT-03 and PE 0603760E, Project CCC-05 to facilitate rapid transition of cyber technologies and laboratory prototypes from applied research to operational prototypes.			
FY 2024 Plans: - Establish a working group with cyber operators from Commands and Services to prioritize cyber technologies and capabilities and initiate technology adaptation and maturation, and collaborative development of operational prototypes. - Coordinate with systems owners to understand the advantages of pipeline and continuous/incremental integration/delivery development models as a means to achieve rapid deployment to operations. - Develop a continuous integration/continuous development pipeline to achieve rapid deployment to operations through continuous authority to operate (cATO).			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Conduct operational test, evaluation, and readiness assessments for operational prototypes in coordination with product owners and approval authorities. ***FY 2025 Plans:*** - Coordinate with cyber operators from Commands and Services to understand evolving needs, prioritize cyber technologies and capabilities, and accelerate technology adaptation and maturation, and collaborative development of operational prototypes. - Assess development pipeline and continuous/incremental integration/delivery processes as a means to achieve rapid deployment to operations. - Assess and refine the continuous integration/continuous development pipeline as a means to achieve rapid deployment to operations through continuous authority to operate (cATO). - Conduct operational test, evaluation, and readiness assessments for operational prototypes in coordination with product owners and approval authorities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects the expansion of efforts to mature, integrate, assess, and transition cyber technologies and laboratory prototypes from applied research to operational prototypes.			
Title: Cyber Agents for Security Testing and Learning Environments (CASTLE)	8.954	16.000	18.000
Description: The Cyber Agents for Security Testing and Learning Environments (CASTLE) program is developing an Artificial Intelligence (AI) toolkit to instantiate realistic network environments and train AI cyber agents to enable resilient network operations against advanced persistent threats (APTs). CASTLE formulates network hardening as a reinforcement learning (RL) problem and teaches RL agents to operate through the post-breach behavior of widely available penetration testing tools. Over progressive rounds of attack and defense, agents explore defensive actions to proactively stop on-going attacks while maintaining operationally relevant workflows. Environments 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 AI cyber agents developed under CASTLE will provide the DoD with continual security assessments of critical networks and real-time response to cyber attacks. ***FY 2024 Plans:*** - Develop approaches for AI cyber agents to devise defensive measures against cyber attacks. - Develop a simulation and execution environment for evaluating cyber agent decision-making and performance. - Develop a library of APT test cases for quantifying cyber agent learning rates, effectiveness, and overhead in realistic DoD network environments. ***FY 2025 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Develop techniques for the automated instantiation of multiple cyber agent training environments for evaluating cyber agent decision-making and performance. - Perform an integrated demonstration of multiple agents defending a realistic network environment. - Extend library of APT test cases and include additional post-breach behaviors as observed in the real-world. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects continued development of reinforcement learning based defensive cyber agents and additional efforts to evaluate their performance.			
Title: Signature Management using Operational Knowledge and Environments (SMOKE) ***Description:*** The Signature Management using Operational Knowledge and Environments (SMOKE) program is developing signature management technologies that generate evasive cyber infrastructure which minimizes signatures as a source of attribution. SMOKE technologies incorporate counter-attribution techniques into the design process; quantitatively measure attribution risk in real-time; and maintain evasiveness after infrastructure changes. SMOKE data-driven tools will automate the planning and execution of threat emulated cyber infrastructure needed for network security assessments by red teams. SMOKE data-driven tools will automate the discovery of cyber threat infrastructure signatures. If successful, SMOKE prototypes will enable red teams to plan, build, and deploy cyber infrastructure that is informed by machine-readable signatures of sophisticated cyber threats. ***FY 2024 Plans:*** - 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 2025 Plans:*** - Develop a fully integrated cyber planning, provisioning, and risk management system that can automatically generate risk-informed cyber infrastructure through real-time, continual attribution assessments. - Integrate cyber planning, generation, and risk management tools with DoD's cyber warfighting architecture and programs of record. - Conduct live demonstrations during DoD cyber exercises to evaluate cyber planning, generation, and risk management tools in collaboration with transition partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:***	21.060	22.000	14.000

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The FY 2025 decrease reflects emphasis shifting from development of signature management technologies to demonstration and performance evaluation in collaboration with transition partners.			
Title: Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)	15.986	15.500	13.000
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 limitation 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 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 coders who are not formal modeling experts. - Establish an initial development, security, and operations-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 2025 Plans:*** - Automate reasoning over models of emergent execution and evaluate their composability at various data granularities for both source code and binaries. - Integrate emergent computation discovery with standard build chains and integrated development environments to provide developer feedback. - Assess the scalability of tools to capture emergent properties and behaviors in complex interactions between multiple layers of abstraction within a subsystem.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Demonstrate the reliability and evaluate the effectiveness of mitigations against unintended system behaviors to reduce military mission risk. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects ramping down of development of tools and continued efforts to demonstrate and evaluate the effectiveness of the tools in mitigating emergent-execution vulnerabilities.			
Title: Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)	19.703	15.400	11.000
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 2024 Plans:*** - Extend user interface to enable understanding of specifications most relevant to component domains and most useful for verification goals. - Develop additional analysis and synthesis tools to increase the percentage of legacy code that can be enhanced. - Develop connections between component interface models and architectural modeling tools to facilitate adoption by developers. - Demonstrate the enhancement of software components for a legacy platform representative of DoD needs. ***FY 2025 Plans:*** - Produce a tool for automated hardware interface exploration of large distributed systems. - Complete development of all analysis and synthesis tools to achieve full coverage of legacy code and demonstrate complete component replacement in a large distributed system. - Integrate tools into a military transition partner platform. ***FY 2024 to FY 2025 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The FY 2025 decrease reflects ramping down of development of technologies and tools for updating legacy code and focus shifting to demonstration and transition of tools to a military partner.			
Title: Business Process Logic (BPL) ***Description:*** The Business Process Logic (BPL) program, addressing issues identified in the Resilient Supply-and-Demand Networks program (budgeted in PE 0602702E, Project TT-13), will develop techniques to characterize and resolve vulnerabilities in business logic systems to protect and assure defense-critical workflows for government and business. Automated workflows written in business logic (BL) control much of the world's enterprises, from administration and operation of seaports to the assembly of weapons systems. Losses due to BL faults and vulnerabilities can range from annoyances to business-threatening outcomes, and so it is important to identify and correct potentially problematic logic issues such as one-way actions or lost resources as early as possible. The BPL program will develop tools to extract workflow representations from BL and use those representations to automatically identify, characterize, and mitigate faults and vulnerabilities in BL scripts and templates. The technologies developed by BPL will enable increased assurance for manufacturing and assembly and greater efficiency for logistics and supply chain management. ***FY 2024 Plans:*** - Formulate machine-processable representations for BL systems that can be generated by ingest of design artifacts and associated documentation. - Explore automated approaches for reasoning across BL representations to characterize faults, trace faults across component interdependencies, and provide mitigations that do not introduce new faults. - Initiate development of a test environment for evaluating the performance of techniques developed for BL representation, analysis, and assurance on representative Defense Industrial Base (DIB) workflows and major BL platforms. ***FY 2025 Plans:*** - Implement machine-processable representations for BL systems and ingest design artifacts and associated documentation. - Demonstrate automated reasoning using BL representations that identifies and characterizes BL faults, traces faults across component interdependencies, and provides mitigations. - Evaluate the performance of techniques developed for BL representation, analysis, and assurance on representative DIB workflows and major BL platforms. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects continued work to develop techniques and tools to characterize and resolve vulnerabilities in business logic systems and additional efforts to evaluate performance of techniques on workflows of importance to the DoD.	-	10.000	19.700
Title: Intelligent Generation of Tools for Security (INGOTS)*	-	9.000	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
Description: *Formerly Automated Assessment of Vulnerabilities (AAV) The Intelligent Generation of Tools for Security (INGOTS) program will develop techniques to identify and triage chainable vulnerabilities within widely used secure computing platforms and assess exploitability. Today, sophisticated cyber attacks link multiple vulnerabilities together into exploit chains that bypass software and hardware security measures to compromise critical, high-value systems. Accurately understanding risk is critical for both developers and defenders within cyberspace, but the metrics currently in use do not account for the multiple factors which differentiate an innocuous software flaw from a chainable vulnerability. INGOTS will develop semi-automated tools and techniques to characterize and measure the interdependent exploitability of vulnerabilities and will pioneer a new vulnerability severity metrology that characterizes and measures interdependent exploitability for the next generation of security vulnerabilities. INGOTS will also develop datasets capturing artifacts and features of vulnerabilities and exploits to further drive program analysis and artificial intelligence (AI) approaches for rapid risk assessment. With the INGOTS vulnerability measurement pipeline, developers and defenders will improve software and hardware resiliency of pervasive commercial systems by rapidly identifying and prioritizing their most dangerous flaws. The INGOTS program is also funded in PE 0602716E, Project ELT-02. ***FY 2024 Plans:*** - Formulate approaches to characterize and measure the interdependent exploitability of vulnerabilities as the basis for a new vulnerability severity metrology. - Develop techniques to accurately quantify the severity of a vulnerability chain in software systems that have state-of-the-art defenses. - Explore and prioritize demonstrations of severity analysis on vulnerabilities of interest to transition partners. ***FY 2025 Plans:*** - Develop and demonstrate techniques to characterize and measure the interdependent exploitability of vulnerabilities in complex software systems. - Quantify the accuracy of vulnerability severity assessment for complex software systems that have state-of-the-art defenses. - Demonstrate the capability to identify and prioritize vulnerabilities in software of interest to transition partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects ramping up of development of techniques to identify and triage chainable vulnerabilities and initial demonstrations of the chainable vulnerability discovery capability.			
Title: Enhanced SBOM for Optimized Software Sustainment (E-BOSS)*	-	6.000	8.014
Description: *Formerly Securing the Software Supply Chain			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The Enhanced SBOM for Optimized Software Sustainment (E-BOSS) program will create enhanced software bill of materials (eSBOM) technologies with new types of rich metadata and develop cyber reasoning algorithms and tools that leverage eSBOMs to defend against potential flaws during the software development process, as well as to triage and remediate flaws found in operation. The global impacts of flawed software deployed at scale (such as the Log4Shell vulnerability found in Log4j cloud and web app deployments, where mitigations took from one week to months, and are not yet completed for a large percentage of systems) motivated the new SBOM requirements in Executive Order 14028. However, standard SBOMs alone cannot enable identification and mitigation of the flow of hostile data to the flaws in the code. E-BOSS will develop software technologies integrated with modern software build chains to enable rapid triage and remediation of vulnerabilities at the scale of national computing infrastructure. The enhanced metadata incorporated in the enhanced eSBOMs will enable trace back of discovered flaw evidence, starting from a crash and walking back through complex inter-component interactions, transfers, and transformations to derive the vulnerability triggers. If successful, E-BOSS technologies will enable cyber-reasoning for improved remediation and sustainment of large scale software systems. The E-BOSS program is funded in PE 0602303E, Project IT-03 and PE 0601101E, Project CCS-02. ***FY 2024 Plans:*** - Formulate enhanced software bill of materials (eSBOM) formats that incorporate new types of rich metadata and initiate development of cyber reasoning algorithms that utilize the information in eSBOMs. - Conceptualize approaches for trace back of discovered flaws, starting from a crash and walking back through complex inter-component interactions, transfers, and transformations to derive the triggers and to identify what and where to apply fixes. ***FY 2025 Plans:*** - Develop eSBOMs with new types of metadata that provide fine-grained data about control and data flows and inter-component interactions and cyber reasoning algorithms and tools that leverage eSBOMs to defend against potential flaws during software development. - Develop algorithms in modern build chains and compiler extensions for unifying program analysis techniques and cyber reasoning tools to enable rapid remediation of vulnerabilities at scale and greater efficiency in software sustainment. - Establish a concept of operations (CONOPS) and design use cases that are relevant to both open source communities as well as to DoD software factories and initiate development of a test and evaluation range architecture extensible to millions of simulated nodes. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects ramping up of development of enhanced SBOM technologies and of use cases and a test range to demonstrate and evaluate security and sustainment benefits on large scale software systems.			
Title: Making and Maintaining in Cyber Security	-	-	24.000

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
Description: Studies conducted under this thrust aim to create and sustain material and cyber capabilities to secure the defense and civilian digital ecosystems. Mathematically based software development techniques, commonly referred to as formal methods, will be created to enable the development and sustainment of provably secure software for civilian and military information systems, cyber-physical and embedded systems, critical infrastructure, and other computation-intensive mission-critical systems. There is a strong interest in tech refresh of legacy software systems through the use of domain-specific and memory-safe languages. Artificial intelligence (AI) and machine learning (ML) will be developed and applied to enhance cyber security and achieve greater operational resilience through cyber monitors and agents that can detect and characterize cyber threats, engage cyber adversaries, prioritize operationally important workflows, maintain essential services, and complete critical missions. ***FY 2025 Plans:*** - Initiate large language model (LLM)-based techniques to automatically rewrite C/C++ code to memory-safe Rust. - Initiate cyber defense techniques for use internal to clouds, including zero-trust techniques to limit damage by adversaries. - Initiate modular development platforms for rapid prototyping and experimentation of integrated hardware-software devices. - Initiate techniques for computer system components to collectively monitor peer components for infection. - Initiate innovative contracting and business processes to enable rapid transition of capabilities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects program initiation.			
Title: Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS)	-	-	20.000
Description: The Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS) program will create scalable mathematically based technologies, tools, and practices to achieve continuous reasoning about complex systems that can support software development pipelines. These mathematically based techniques, or formal methods, enable rigorous modeling, reasoning, and proving diverse properties of software code or design models, for example, the absence of a specific type of defect or security vulnerability. PROVERS integrates formal methods into a modern incremental and iterative development process by running tools at each code commit and delivering results to developers when they can most effectively remediate discovered issues. To achieve this, PROVERS will focus on creating and sustaining a body of evidence that can co-evolve with the system under change to support continuous assessment and ensure that the system remains free of identified categories of defects and security vulnerabilities through its lifetime. Key PROVERS objectives include enabling proof maintenance and repair capabilities at a cost that is proportionate to code change; integration of formal methods with code, properties, and proofs in a single workflow that reduces human involvement; providing improved explanations to facilitate proof repair; and automating formal methods-based software analysis to support software developers that are not formal methods experts. PROVERS technologies will facilitate the agile development and continuous improvement of mission-critical software systems that meet the high security and quality standards required by the DoD. Basic research for this program is funded in PE 0601101E, Project CCS-02.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
FY 2025 Plans: - Create advanced techniques for proof engineering, including knowledge, methods, and tools, that are readily accessible to software engineers. - Design proof-friendly software development systems that facilitate the formal verification of a broad range of system properties in a single workflow that reduces human involvement. - Formulate quantitative models to establish that proof maintenance and repair capabilities are provided at a cost that is proportionate to code change. - Perform security assessments of developed codes for high-assurance systems. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects the initiation of applied research to develop, demonstrate, and evaluate scalable techniques and formal methods to enable continuous reasoning about complex systems that can support software development pipelines.			
Title: Open, Programmable, Secure 5G (OPS-5G)	20.791	18.500	-
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 is coordinating with existing open-source 5G efforts and U.S. Government, DoD, and industry stakeholders. ***FY 2024 Plans:*** - Extend security architectures capable of defending Internet of Things (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 2024 to FY 2025 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The FY 2025 decrease reflects program completion.			
Title: Program Analysis for Capability Excellence (PACE)	17.465	8.500	-
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 2024 Plans:*** - Demonstrate the versatility of the system by increasing the complexity of the software under attack and the sophistication of the simulated attacker and assess system performance against both automated adversaries and human experts. - Collaborate with transition partners to improve and further develop systems to identify and mitigate software compromise. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects program completion.			
Title: Assured Micropatching (AMP)	19.910	7.500	-
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 is creating capabilities 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 the DoD depends. ***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 2024 to FY 2025 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The FY 2025 decrease reflects program completion.			
Title: Fast Network Interface Cards (FastNICs) ***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 2024 Plans:*** - Extend machine learning algorithms to increase hardware utilization and reduce power consumption. - Demonstrate hybrid optical-electrical network interface and computation hardware to support machine learning. - Augment machine learning applications to operate over DoD and commercially available network topologies. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects program completion.	12.187	5.999	-
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 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 2024 Plans:*** - 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 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects program completion.	19.902	5.060	-
Title: Resilient Anonymous Communication for Everyone (RACE)	8.800	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
Description: The Resilient Anonymous Communication for Everyone (RACE) program developed cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient, mobile communications within a network environment. RACE developed 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 maintained confidentiality, integrity, and availability of messaging while preventing large-scale compromise of the system. RACE security was based on rigorous security arguments or statistical arguments based on realistic simulations, and not on ad hoc estimates of security.			
Title: Memory Optimization (MemOp) ***Description:*** The Memory Optimization (MemOp) program developed 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 were 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 explored 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 were implemented and evaluated in hardware and software. The technologies developed in MemOp provide enhanced efficiency and improved performance for large scale computing systems.	7.007	-	-
Title: Cyber-Hunting at Scale (CHASE) ***Description:*** The Cyber-Hunting at Scale (CHASE) program developed 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 developed 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.	6.450	-	-
Title: Searchlight ***Description:*** The Searchlight program developed 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 developed novel approaches for allocating inherently limited network resources to optimize the performance of distributed applications. Searchlight techniques and systems enabled	5.747	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
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.			
Title: Computers and Humans Exploring Software Security (CHESS) ***Description:*** The Computers and Humans Exploring Software Security (CHESS) program developed 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 envisioned a future in which high-intensity cyber operations are conducted by computer-human teams. CHESS capabilities were 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 required innovative combinations of automated program analysis techniques with support for mixed-initiative computer-human collaboration. CHESS aimed 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.	5.000	-	-
Accomplishments/Planned Programs Subtotals	220.380	167.459	185.714

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency			Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	131.883	150.570	164.747	-	164.747	188.155	211.747	223.875	231.844	-	-

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 2023	FY 2024	FY 2025
Title: Assured Neuro Symbolic Learning and Reasoning (ANSR)	9.620	14.000	16.500
Description: The Assured Neuro Symbolic Learning and Reasoning (ANSR) program is developing new hybrid artificial intelligence (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 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Develop initial use cases and an architecture for engineering and demonstrating mission relevant applications of hybrid AI algorithms. ***FY 2025 Plans:*** - Develop hybrid AI approaches that iteratively reason over symbolic and neural representations for perception, planning, and control to enable enhanced situational understanding, activity recognition, and safety in maneuvering. - Develop an assurance test harness with adversarial AI and evaluate the new hybrid algorithms and architectures. - Perform initial demonstration and evaluation of hybrid AI technologies and their composition in use cases of interest to the DoD. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects ramping up of development of techniques that integrate symbolic reasoning with data-driven machine learning and initiation of demonstration and evaluation on high priority use cases of interest to the DoD.			
Title: Accelerating Artificial Intelligence (AAI)	30.101	30.365	13.250
Description: The Accelerating Artificial Intelligence (AAI) program seeks to go beyond commercially-driven advances in artificial intelligence (AI) and to address important national security challenge applications. Trustworthy AI, which is AI that is safe, reliable, accurate, explainable, and resilient to attacks, is a major focus. Technical challenges include robustness of AI systems in novel, uncertain, and/or unanticipated situations; efficiency and timeliness of AI development, test, evaluation, approval, and certification processes; and identification of tasks or sub-tasks for which greater automation through the use of artificial intelligence/machine learning (AI/ML) is appropriate. Approaches to addressing these challenges will leverage recent advances in transfer learning, causal reasoning, reinforcement learning, generative AI, and large pre-trained models (LPTMs) and large language models (LLMs). If successful, AAI will significantly accelerate AI innovation in many important DoD domains while also reducing the time and cost needed to transition and deploy new AI technologies. ***FY 2024 Plans:*** - Refine methods for converting interview questions into stimuli that evoke preconscious neural and physiological responses. - Develop strategies to mitigate variables that confound the data collection process necessary for aggregating an individual's preconscious response to stimuli. - Develop digital twins representing diverse sets of human teammates for scalable modeling and quantitative assessment of human-AI interaction in realistic settings. - Establish and construct AI technologies, 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 2025 Plans:*** - Assemble data acquisition systems that synchronize physiological monitoring of both peripheral sensing (e.g., pupil, cardiac monitoring) and neural sensors (e.g., electroencephalogram).			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Conduct initial real-time tests of machine learning/AI algorithm architectures for analyzing preconscious information evoked by behavioral health related stimuli. - Evaluate potential of using open-source, deidentified, health-related databases to reduce the need for personalized calibration data when training machine learning architectures for analyzing preconscious information evoked by behavioral health related stimuli. - Demonstrate AI technologies, engineering, and human-machine teaming approaches that enable trustworthy AI for mission- and safety-critical domains. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects a shift from heavy development of techniques and testing environments to demonstration and test execution.			
Title: Learning Introspective Control (LINC)	8.510	23.000	9.497
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 2024 Plans:*** - Demonstrate computational efficiency of control reconstitution algorithms and establish suitability for integration in DoD systems that have limited spare computational resources. - Integrate 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. - Using representative platforms, perform experiments that demonstrate recovery and control of cyber-physical systems for high-priority use cases in collaboration with transition partners. ***FY 2025 Plans:*** - Extend system modeling and control techniques to additional platform types. - Collect performance measurements from platform experiments and demonstrate the ability to maintain functionality in the presence of damage or malfunction, without pre-training or prior modeling.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Conduct field experiments involving recovery and control of cyber-physical systems for high-priority use cases in collaboration with transition partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects shift from development and implementation of learning introspective control techniques to experimentation involving high-priority use cases in collaboration with transition partners.			
Title: Artificial Intelligence Cyber Challenge (AIxCC)	-	25.000	39.000
Description: The Artificial Intelligence Cyber Challenge (AIxCC) program, addressing issues encountered in the Program Analysis for Capability Excellence (PACE) program (budgeted in PE 0602303E, Project IT-03), seeks to develop and demonstrate techniques for automated discovery and remediation of software vulnerabilities at speed and at scale to secure widely used, critical code. Current automated vulnerability discovery and remediation tools are based on techniques such as fuzzing, logical reasoning, and genetic algorithms, but are limited in terms of effectiveness and user support. AIxCC will leverage recent dramatic advances in artificial intelligence (AI) and machine learning, such as large pre-trained models (LPTMs) and neurosymbolic AI, as the basis for new automated cyber security technologies and tools. AIxCC will use a contest model where teams will use their automation and tooling to complete vulnerability discovery and remediation challenges. Performer teams will be selected for the AIxCC competition based on their capability to leverage advances in AI to create usable, automated tools for vulnerability discovery and remediation, with a focus on tools suitable for broad deployment and applicable to critical infrastructure sectors. AIxCC competitors will train and develop their systems to find and fix vulnerabilities in widely-used open source software, focusing on software used in critical infrastructure. Each competitor system will be evaluated on real-world critical infrastructure software suites and will be scored based on their results both in terms of absolute performance and performance relative to other competitor systems. Winning teams will receive cash awards. If successful, AIxCC will create novel AI-enabled cyber vulnerability remediation technology and tools for securing code at the scale and speed needed to defend U.S. critical infrastructure from cyber attacks. ***FY 2024 Plans:*** - Formulate cyber competitions involving vulnerability discovery and remediation for open source software used in critical infrastructure. - Construct a distributed platform for conducting cyber competitions. - Devise scoring schemes that accurately reflect the effectiveness of automated AI-based vulnerability discovery and remediation systems when applied to the software used in critical infrastructure. - Conduct an initial AI-based vulnerability discovery and remediation cyber challenge focused on critical infrastructure software. ***FY 2025 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Develop more advanced cyber competitions involving AI-based vulnerability discovery and remediation for software used in critical infrastructure. - Expand the platform for conducting cyber competitions. - Refine scoring schemes to more accurately reflect the effectiveness of automated AI-based vulnerability discovery and remediation systems when applied to the software used in critical infrastructure. - Conduct a final AI-based vulnerability discovery and remediation cyber competition focused on critical infrastructure software. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects continued development of automated AI-based vulnerability discovery and remediation techniques and increased efforts to evaluate the technology on critical infrastructure software.			
Title: Open Price Exploration for National security (OPEN)	-	16.000	30.000
Description: The Open Price Exploration for National security (OPEN) program aims to increase supply chain resilience and enable more efficient critical mineral markets by leveraging advances in artificial intelligence (AI) prediction and forecasting to increase price, supply, and demand transparency. Based on concepts developed in the LogX Program (budgeted in PE 0603760E, Project CCC-02), OPEN will construct structural price predictions from fundamental and observable critical mineral input costs and increase the accuracy and precision of supply and demand forecasts by leveraging this structural price in conjunction with advances in AI and economic modeling. Today, critical mineral markets and supply chains are vulnerable. International supply shocks can lead to large and rapid critical mineral price spikes with immediate economic ramifications, and commodities purchase transactions (e.g., offtake agreements) are negotiated leveraging a mix of opaque and flawed pricing data. OPEN will leverage a decomposition of a critical mineral price into four components (input costs, supply/demand shocks, distortions due to noncompetitive behavior, and stochastic fluctuation) to construct transparent estimations of an approximate marginal cost for critical minerals indexed by time and geographic location, and will estimate supply and demand forecasts for critical minerals that take into account geopolitical factors, energy fluctuations, and technological innovations in recycling and supply chain management. Technology developed under this program will transition to the Services and commercial partners. ***FY 2024 Plans:*** - Develop data engineering framework for acquisition, aggregation, fusion, and provision of data. - Select initial critical minerals. - Construct structural price prediction models. - Construct supply and demand forecasting models. ***FY 2025 Plans:*** - Expand scope of critical minerals. - Evaluate models to assess operational relevance to transition partners.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Update and improve performance of structural price prediction models. - Update and improve performance of supply and demand forecasting models. - Explore extension of model architecture to additional classes of materials. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects a shift from initial development to testing and updating models.			
Title: Transfer from Imprecise and Abstract Models to Autonomous Technologies (TIAMAT)*	-	10.000	17.000
Description: *Formerly Learning Autonomy in Synthetic Environments (LASE) The Transfer from Imprecise and Abstract Models to Autonomous Technologies (TIAMAT) program will develop techniques to robustly transfer learned autonomy from fast abstract simulations to autonomous platforms in real-world environments. The autonomy levels of unmanned systems of today are limited because the modeling and simulation (M&S) training environments do not account for the data domain shift common when translating M&S outcomes to the real world - this phenomenon is sometimes referred to as the sim2real gap. The TIAMAT approach will integrate symbolic structures with neural structures to more realistically and robustly transfer learned autonomy. TIAMAT will enable the use of fast abstract simulations by anchoring the learning and transfer of autonomy on semantically consistent components shared across simulations and real environments, so-called "semantic anchors". For TIAMAT, semantic anchors of particular importance include those militarily-relevant phenomena that remain consistent in the source and target environments, for example, mission objectives, special instructions, subject matter expert guidance, rules of engagement, and the laws of physics. Autonomy transfer using semantic anchors will reduce the complexity of the autonomy learning and transfer problems to the comparatively simpler points of reference in the anchored representation. If successful, TIAMAT transfer of M&S-based learning will enable more rapid and robust training and deployment of autonomous systems at higher levels of autonomy. ***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 architecture for evaluating performance of transfer learning of autonomy using semantic anchors. ***FY 2025 Plans:*** - Develop a framework for assessing the robustness to the sim2real gap of autonomy transfer from fast, abstract simulations that are available or can be quickly or automatically developed for a given use case. - Develop techniques to leverage semantic anchors for use in a rapid, robust, autonomy transfer learning system.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Demonstrate an initial capability to transfer autonomy from readily available or quickly developed abstract simulations to live platforms for scenarios of interest to military operators and potential transition partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects ramping up of development of techniques to robustly transfer learned autonomy from fast abstract simulations to autonomous platforms for scenarios of interest to military operators and potential transition partners.			
Title: Access in AI and Human-Machine Symbiosis ***Description:*** Studies conducted under this thrust aim to advance core artificial intelligence (AI), human-machine symbiosis (HMS), and machine learning (ML) technologies that ensure physical or virtual presence where and when necessary to provide knowledge and/or achieve desired effects. Primary considerations include the safety, trustworthiness, and security of AI/HMS/ML as an adjunct to human operators and analysts. The potential for AI/HMS/ML systems to leak sensitive/classified training data is of concern, particularly for large language models and large pre-trained models (LPTMs). Another focus involves the human-AI interaction, including techniques to ensure that the human correctly understands the output from the AI/HMS/ML system. This thrust addresses the current limitations of AI/HMS/ML-based technologies to enable implementation in mission-critical information systems suitable for military use. ***FY 2025 Plans:*** - Initiate development of chatbots capable of realistic and positive dialog. - Initiate designs for LPTMs supplemented with legal sources to propose legal actions to deter adversaries. - Initiate exploration of mechanisms to enable rapid transition of intelligence capabilities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects program initiation.	-	-	13.000
Title: Making and Maintaining in AI and Human-Machine Symbiosis ***Description:*** Studies conducted under this thrust aim to develop artificial intelligence (AI), human-machine symbiosis (HMS), and machine learning (ML) technologies to facilitate the creation and sustainment of physical and cyber capabilities. AI/HMS/ML-based abstractions, patterns, architectures, assurance techniques, and iterative processes are developed to facilitate the creation and sustainment of complex systems that must rely on AI-based components and associated training data. The capability to engineer AI/HMS/ML systems that meet the safety, trustworthiness, integrity, and security requirements for mission-critical applications will provide great benefit to the DoD and commercial industry. ***FY 2025 Plans:*** - Initiate exploration of approaches for assuring the integrity of large language models and large pre-trained models (LPTMs). - Initiate development of user protection layers to enable safe and secure mixed reality systems.	-	-	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Initiate development of negotiation chatbots to enable rapid, iterative, and comprehensive wargaming of complex scenarios. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2025 increase reflects program initiation.			
Title: Awareness in AI and Human-Machine Symbiosis ***Description:*** The changing landscape of R&D development with renewed great power competition and increased commercial investment means that the DoD must maintain awareness of rapidly changing technology areas in fundamentally different ways. Artificial intelligence (AI) enabled systems permeate everyday life, and commercial AI development is advancing rapidly. Therefore, DoD must maintain awareness of the implications and opportunities of these technologies for defense and National Security applications, broadly defined to include how societal changes may affect adversary approaches to competition. DoD must also understand which unique defense and military needs will not be well supported by commercial AI development. For instance, the novelty and unique contextual situations military systems are required to operate in are not well represented in current commercial training data sets, making it highly unlikely that the way industry is approaching the problem will result in AI that adequately addresses defense applications. Focus areas include new approaches for empowering AI and AI-enabled systems to adapt to varied environments, and for enabling AI reasoning. ***FY 2025 Plans:*** - Investigate the potential of AI language processing to enable abstract reasoning. - Initiate the development of capabilities for generalizable knowledge representation and reasoning. - Initiate development of techniques to enable transparent and logical communications between humans and AI models. - Initiate development of methods for computing attitudes of foreign populations. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 increase reflects program initiation.	-	-	9.500
Title: Warfighting Performance in AI and Human-Machine Symbiosis ***Description:*** Studies conducted under this thrust aim to ensure the operational reliability and effectiveness of human, physical, and cyber systems that incorporate artificial intelligence (AI), human-machine symbiosis (HMS), and machine learning (ML) technologies and capabilities. Future advances in AI/HMS/ML will require hybrid designs and learning processes that are influenced both by training data and by key concepts and features proposed by experts in the intended application domains. Such hybrid approaches provide robustness against adversarial attack and improve human alignment. AI/HMS/ML evaluation and assurance is an on-going challenge, and so new techniques, tools, and practices are developed for verifying and validating AI/HMS/ML-based systems that are capable, safe, secure, trustworthy, affordable, and timely, especially for large language models and large pre-trained models (LPTMs).	-	-	7.000

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
FY 2025 Plans: - Initiate multi-level security architectures, technologies, and concepts of operations (CONOPS) for LPTMs. - Initiate AI algorithms and LPTM architectures that can resist security challenges and mitigate attack consequences. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2025 increase reflects program initiation.			
Title: Automating Scientific Knowledge Extraction and Modeling (ASKEM)	13.130	19.000	-
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 2024 Plans:*** - Establish baselines and measure technical component performance for accuracy, timeliness, maintainability, and scalability in selected evaluation domains. - Implement and test interfaces and components, develop 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. - Evaluate the workbench against diverse use cases across the modeling and simulation lifecycle in collaboration with transition partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
The FY 2025 decrease reflects program completion.			
Title: Automated Rapid Certification Of Software (ARCOS)	17.930	8.200	-
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 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 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects program completion.			
Title: Assured Autonomy	5.150	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 the DoD to more rapidly and efficiently deploy learning-enabled autonomous systems that can be trusted to operate safely in uncertain environments. ***FY 2024 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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 2023	FY 2024	FY 2025
- Transition integrated toolchain and assurance tools to DoD partners. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY 2025 decrease reflects program completion.			
Title: Knowledge-directed Artificial Intelligence Reasoning Over Schemas (KAIROS) ***Description:*** The Knowledge-directed Artificial Intelligence (AI) Reasoning Over Schemas (KAIROS) program developed 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 developed 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.	24.511	-	-
Title: Symbiotic Design ***Description:*** The Symbiotic Design program developed 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 addressed 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 created technologies essential for AI co-design: design space construction, design composition, and design space exploration. The program demonstrated the approach at realistic scales by a sequence of CPS design challenges of increasing complexity, and quantified the results with respect to development time, system performance, quality, and innovation metrics.	22.931	-	-
Accomplishments/Planned Programs Subtotals	131.883	150.570	164.747

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2025 Defense Advanced Research Projects Agency		Date: March 2024
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*

D. Acquisition Strategy

N/A