Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Defense Advanced Research Projects Agency	Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
Total Program Element	-	416.935	420.920	430.363	-	430.363	-	-	-	-	-	-
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	14.250	6.576	0.000	-	0.000	-	-	-	-	-	-
IT-03: *CYBER SECURITY*	-	262.861	236.182	237.089	-	237.089	-	-	-	-	-	-
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	139.824	178.162	193.274	-	193.274	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

The Information and Communications Technology Program Element is budgeted in the Applied Research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies. This Program Element also supports innovation and robust transition planning in the technology cycle by working with entrepreneurs to increase the likelihood that DARPA funded technologies take root in the U.S. and provide new capabilities for national defense.

The High Productivity, High-Performance Responsive Architectures project focuses on developing the computer hardware and associated software technologies required for future computationally- and data-intensive national security applications. Powerful new approaches are needed to manage the rapid growth in available sensor data, to leverage advances in machine learning and artificial intelligence, and to maintain the security of DoD information systems.

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

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

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Defense Advanced Research Projects Agency	Date: May 2021
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602303E *I INFORMATION & COMMUNICATIONS TECHNOLOGY*

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	428.556	435.920	454.599	-	454.599
Current President's Budget	416.935	420.920	430.363	-	430.363
Total Adjustments	-11.621	-15.000	-24.236	-	-24.236
• Congressional General Reductions	0.000	-15.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.619	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	-4.729	0.000			
• SBIR/STTR Transfer	-7.511	0.000			
• TotalOtherAdjustments	-	-	-24.236	-	-24.236

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2020	FY 2021
Project: IT-03: *CYBER SECURITY*		
Congressional Add: *Distributed Ledger Technology*	1.000	-
Congressional Add Subtotals for Project: IT-03	1.000	-
Congressional Add Totals for all Projects	1.000	-

Change Summary Explanation

FY 2020: Decrease reflects the SBIR/STTR transfer and reprogrammings offset by COVID response CARES Act add.

FY 2021: Decrease reflects congressional adjustments.

FY 2022: Decrease reflects the completion of the IT-02 High Productivity, High Performance Responsive Architectures project, and the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) cyber security program.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	14.250	6.576	0.000	-	0.000	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project focuses on developing the computer hardware and associated software technologies required for future computationally- and data-intensive national security applications. Powerful new approaches are needed to manage the rapid growth in available sensor data, to leverage advances in machine learning and artificial intelligence, and to maintain the security of DoD information systems. The project therefore aims not only to create larger computing platforms but also to efficiently extract information out of large and chaotic data sets with embedded and low-size, weight, and power systems. Advances in these areas will allow DoD electronic systems to collaboratively manage scarce resources, such as the electromagnetic spectrum, and to adapt to new requirements and situations. Further, the resulting technologies, by being accessible to a wide range of application developers, will support new, sustainable computing systems for a broad spectrum of scientific and engineering applications.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: RF Machine Learning Systems (RFMLS)	14.250	6.576	-
Description: The RF Machine Learning Systems (RFMLS) program is addressing the performance limitations of conventional radio frequency (RF) systems such as radar, signals intelligence, electronic warfare, and communications. The performance of future RF systems in the DoD will be defined by their ability to adapt and respond to their environment in real-time. We currently lack both the algorithms and computational power to manage the volume of data and complexity of decision-making that will be required. RFMLS technology will develop machine learning techniques that are able to help manage this complexity, for example, by recognizing specific emitters or detecting anomalies in a cluttered environment. The objective of the RFMLS program is to both develop these foundational technologies and to apply them to relevant DoD systems. ***FY 2021 Plans:*** - Complete final phase development of machine learning algorithms and architectures for all four of the challenge problems. - Complete a real-time, open-air demonstration of RFMLS capabilities. - Transition technology applications to relevant partners. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects program completion.			
Accomplishments/Planned Programs Subtotals	14.250	6.576	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
IT-03: *CYBER SECURITY*	-	262.861	236.182	237.089	-	237.089	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Intent-Defined Adaptive Software (IDAS)	8.000	14.100	17.350
Description: The Intent-Defined Adaptive Software (IDAS) program is developing technologies to represent the intent of software and its abstract constraints separately from its concrete instantiation, for the purpose of enabling rapid code synthesis and continual adaptation. Modern weapons platforms are increasingly dependent on complex software, increasing the risk of system failures and creating new attack surfaces for adversaries. Software engineers often manage complexity by choosing a particular option that fulfills the immediate needs of the development effort (e.g., by concretization). IDAS will develop techniques for deferring software concretizations until uncertainties are resolved, either at build time or during run time, for complex systems. IDAS technology aims to significantly reduce software development time and maintenance costs, thereby enabling DoD to acquire, sustain, and improve software-based capabilities more cost-effectively.			
FY 2021 Plans: - Develop algorithms for deferring software concretizations until uncertainties are resolved for complex logistics, machine-learning, and cloud software systems. - Develop techniques that permit optimization of multiple implementations, and enable more efficient encoding of quality goals and operational constraints. - Test and evaluate alternative software synthesis algorithms for automated modification by rapidly revising the representation of the intent of the software and measuring software maintenance effort.			
FY 2022 Plans: - Select, scale, optimize, and increase the robustness of the highest performing algorithms for deferring software concretizations in complex logistics, machine-learning, and cloud software systems.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Mature algorithmic techniques that permit verified optimization of multiple implementations, and demonstrate more efficient encoding of quality goals and operational constraints. - Demonstrate initial transitionable capabilities of the highest performing alternative software synthesis algorithms for automated modification of representative military software systems and quantify software maintenance effort. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects continued development and implementation of techniques for deferring software concretization, and increased work to demonstrate and evaluate alternative approaches in the context of representative military software systems.			
Title: Memory Optimization (MemOp)	19.060	18.000	17.000
Description: The Memory Optimization (MemOp) program is developing technology to optimize memory transactions in large scale computing systems. The demand for computing services is growing within both the U.S. Government and commercial industry. In response, new technical approaches are being developed to provide massive computation efficiently and cost effectively. In particular, distributed data centers with high-speed interconnects and customizable hardware, including graphics processing units (GPU) and field programmable gate arrays (FPGAs), are being used by service providers to achieve greater efficiency and improved processing performance. MemOp is exploring new memory architectures that more fully leverage emerging customizable hardware to deliver computing services reliably and at reduced cost. The more promising MemOp memory architectures will be implemented and evaluated in hardware and software. The technologies developed in MemOp will provide enhanced efficiency and improved performance for large scale computing systems. ***FY 2021 Plans:*** - Enhance the scalability of algorithms for task mapping in large scale memory systems, and optimize software implementations. - Implement and test methods to interface to memory and accelerated processing pipelines. - Leverage the testbed to evaluate memory transaction improvements in systems incorporating GPUs and FPGAs. - Optimize algorithms and architectures for memory transaction performance in hardware and software, and evaluate on testbed. ***FY 2022 Plans:*** - Refine and leverage algorithm scaling for task mapping in large scale memory systems, and optimize software implementations. - Evaluate and refine integration of memory and accelerated processing pipelines. - Evaluate memory transaction implementation and develop improvements on program testbed. - Optimize algorithms and architectures for memory transaction performance in hardware and software, and evaluate on testbed. ***FY 2021 to FY 2022 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
The FY 2022 decrease reflects ramping down of development of memory interface methods and accelerated processing pipelines, and continued development and use of an enhanced evaluation testbed.			
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 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 2021 Plans:*** - Build efficient ZK proof generation compilers optimized for large and complex problem statements, and that can operate in an efficient manner. - Extend post-quantum analyses to important cases such as non-interactive zero knowledge from post-quantum assumptions, and zero knowledge from symmetric key primitives. - Validate the functionality, information leakage potential, and robustness to attack of developed ZK techniques and software on a set of DoD-relevant applications. ***FY 2022 Plans:*** - Extend ZK proof compilers by adding problem classes as well as reducing representation size of proof statements by orders of magnitude. - Optimize post-quantum analyses to reduce theoretical proof complexity for important use cases. - Enhance techniques to permit optimization for any subset of prover computation, verifier computation, total communication, and total number of communication rounds. - Apply ZK proof techniques to additional DoD and U.S. Government use cases and evaluate their functionality, information leakage potential, and robustness to attack in collaboration with potential transition partners. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects continued development of cryptographic technologies and increased efforts to extend and validate their functionality, information leakage potential, and robustness to attack on applications of interest to the DoD.	7.700	14.500	16.000
Title: Cyber-Hunting at Scale (CHASE)	19.000	16.140	15.100

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
Description: The Cyber-Hunting at Scale (CHASE) program is developing data-driven tools for real-time cyber threat detection, characterization, and protection within enterprise-scale networks. U.S. computer networks are continually under attack, but at present there are few capabilities to efficiently extract and analyze the right data from the right device at the right time for DoD-scale information networks. For example, analysis of an in-memory exploit requires detailed data from a few devices, while analysis of a global botnet attack requires summary data from a great many devices. CHASE is developing novel algorithms and analysis tools to dynamically collect data from across the network, actively hunt for advanced threats that evade routine security measures, and automatically disseminate protective measures that bolster the collective cyber defense posture. ***FY 2021 Plans:*** - Evaluate threat detection, threat characterization, and data planning feedback loops at enterprise scale, and demonstrate ability to adapt sensor feeds based on threat characterizations. - Evaluate ability for threat detection and characterization to improve detection accuracy and reduce the time analysts require to diagnose alerts. - Evaluate the extent to which novel data retention policies can improve detection accuracy while reducing the amount of historic data stored. - Quantitatively characterize how the accuracy of global cross-enterprise threat detection depends on data policies. ***FY 2022 Plans:*** - Develop an analyst interface to enable automated cyber report generation, evaluate the utility of the interface, and demonstrate foundational protective measures given specific threat detections. - Develop and demonstrate techniques for quantifying the risk of cyber operations. - Identify transition opportunities for validated threat detection, threat characterization, and data planning algorithms. - Integrate threat detection, data retention, and global analysis methods, and harden capabilities for transition to DoD stakeholders. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease is the result of development and integration work decreasing, and the focus shifting to demonstration, hardening, and transition to DoD stakeholders.			
Title: Resilient Anonymous Communication for Everyone (RACE)	12.700	13.500	14.700
Description: The Resilient Anonymous Communication for Everyone (RACE) program is developing cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient, mobile communications within a network environment. RACE is developing a mobile phone application and distributed systems that provide a secure message-passing service by combining advances in distributed system tasking with communication protocol encapsulation methods. The RACE system will maintain confidentiality, integrity, and availability of messaging while preventing large-scale compromise of the system.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
RACE security is based on rigorous security arguments or statistical arguments based on realistic simulations, and not on ad hoc security claims. ***FY 2021 Plans:*** - Refine and scale up the secure message-passing system by improving the efficiency of techniques for computing on encrypted routing information. - Integrate components into a secure message-passing system to defeat a cyber adversary with limited ability to observe the network by making the communication protocols statistically indistinguishable from legacy protocols. - Enhance the testbed and demonstrate the integrated secure message-passing system against an active simulated cyber adversary that seeks to discover the obfuscation and cryptographic technologies while possessing limited knowledge of the system. ***FY 2022 Plans:*** - Enable the system to scale to thousands of users by improving the efficiency of techniques for computing on encrypted routing information. - Integrate enhanced components into the secure message-passing system with improved capability to counter a cyber adversary who has access to communication protocol information and communication nodes. - Enhance the testbed and demonstrate the integrated secure message-passing system against a simulated cyber adversary that has full knowledge of the system. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects continued development of obfuscation and encryption technologies, continued implementation of a secure message-passing system and testbed, and expanded work to evaluate the system against a simulated cyber adversary.			
Title: Assured Micropatching (AMP) ***Description:*** The Assured Micropatching (AMP) program is developing technologies to enable the rapid production of targeted micropatches to repair legacy program binaries with strong guarantees. At present, the emergency patching of legacy software, even if all relevant information is available, takes far too long, leaving critical systems with known flaws vulnerable to adversary attack. AMP will create the capability to analyze, modify, and fix legacy software in binary form even when the original source code and/or build process is not fully available. The AMP technical approach involves automatic discovery of known vulnerable components, goal-driven decompilation to isolate and analyze the vulnerable binary components, and minimal-change patching and recompilation to rebuild affected binaries with strong guarantees that the patch will not impair the functions of the system. The technologies developed by AMP aim to enable cyber defenders to quickly and accurately patch legacy binaries in the deployed software systems upon which our military depends.	12.400	16.410	13.500

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2021 Plans: - Develop prototype goal-driven decompilers, and demonstrate feasibility of iteratively guiding decompilation with fitness functions relevant to repairing binary flaws. - Develop prototype recompilers that produce both a micropatch and a formal representation of the effects of the micropatch suitable for use in a proof that the effects of the patch are isolated from other components. - Perform initial tests of decompiler and recompiler prototypes on at-scale system binaries. ***FY 2022 Plans:*** - Develop supergraph generator to infer compiler optimization effects on the call graph structure. - Develop probabilistic graph-matching and inference algorithms to produce candidate matches between the target binary procedures and most likely source code procedures. - Create a Ghidra extension to interactively show the effects of an applied micropatch. - Conduct a challenge event using a commodity Controller Area Network (CAN) controller/data logger based on a widely-used commercial architecture. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of work to develop prototype decompilers and recompilers, and focus shifting to work to demonstrate the technology on realistic challenge problems.			
Title: Computers and Humans Exploring Software Security (CHESS)	18.000	14.375	12.400
Description: The Computers and Humans Exploring Software Security (CHESS) program is developing technologies to enable computers and humans to reason collaboratively over software artifacts, such as source code and compiled binaries, with the goal of finding vulnerabilities more rapidly and accurately than unaided human operators. CHESS envisions a future in which high-intensity cyber operations are conducted by computer-human teams. CHESS capabilities will be designed for use by humans of varying skill levels, even those with minimal previous cyber experience or relevant domain knowledge. Achieving the necessary scale and timelines in vulnerability discovery will require innovative combinations of automated program analysis techniques with support for mixed-initiative computer-human collaboration. CHESS aims to enable U.S. operational cyber superiority by combining human-generated insight into the vulnerability discovery process with the speed and scale of computational analysis. ***FY 2021 Plans:*** - Implement and demonstrate techniques for emitting a proof of vulnerability to confirm existence of a vulnerability, and for generating a non-disruptive, specific patch to neutralize the vulnerability. - Expand cyber reasoning techniques to discover additional classes of software vulnerabilities, and enhance representations of information gaps revealed by expanded cyber reasoning techniques.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Demonstrate an end-to-end, integrated computer-human software reasoning system to DoD and Intelligence Community (IC) transition partners. ***FY 2022 Plans:*** - Scale techniques for emitting a proof of vulnerability to confirm existence of a vulnerability, and for generating a non-disruptive, specific patch to neutralize the vulnerability, to programs of the size and complexity found in military systems. - Enhance representations of information gaps revealed by expanded cyber reasoning techniques to enable non-experts in vulnerability discovery to approach expert-level efficacy. - Incorporate improved cyber reasoning capabilities and additional operator-requested refinements in an end-to-end, integrated computer-human software reasoning system for the DoD and IC. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of work to integrate technologies in a proof-of-concept, computer-human software reasoning system, and focus shifting to enhancement, demonstration, and transition to the DoD and IC.			
Title: Fast Network Interface Cards (FastNICs)	6.900	12.000	11.500
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 iterative training of machine learning systems. ***FY 2021 Plans:*** - Extend the most widely used distributed systems software and operating systems to accommodate massively parallel input data streams. - Implement alternative architectures for the network interface, and quantify achievable communications bandwidth and processing throughput. - Implement distributed computing applications, such as machine learning, that effectively utilize massively parallel data streams. ***FY 2022 Plans:*** - Evaluate network interface architecture alternatives such as busses and parallelism. - Demonstrate versions of widely used distributed systems software and operating systems that accommodate massively parallel input data streams.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Demonstrate and evaluate distributed computing applications of interest to the DoD such as training deep learning systems. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of work to implement improved network interfaces, and focus shifting to demonstration and evaluation on distributed applications of interest to the DoD.			
Title: Cora ***Description:*** The Cora program is developing technologies to enable machines to read heterogeneous text-based data sources, extract key entities and activities, and characterize cyber threats. Large volumes of text-based data contain scattered clues about the activities of cyber threats. Automated machine reading and analysis capabilities are required due to the extreme rates at which this text-based data is generated. In addition, the connections between extracted entities and their activities can be very subtle and, because they are buried in noise, difficult to detect and correlate. The Cora technologies will benefit cyber analysts by providing them with pre-processed cyber leads that otherwise might not be available. ***FY 2021 Plans:*** - Evaluate cyber analytical technologies on large-scale data, and implement algorithmic improvements to address scalability and performance. - Develop natural language understanding capability in text-based data other than English. - Provide initial software capabilities to transition partners for performance assessments in operational environments. ***FY 2022 Plans:*** - Demonstrate scalability and performance of analytical capabilities on relevant large-scale data sets. - Evaluate machine-learning-based methods for identifying cyber threats across heterogeneous data, in multiple languages. - Harden cyber analytical software technologies and incorporate refinements requested by cyber operators. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of efforts to implement and evaluate an integrated cyber analytical system, and transition to operational partners.	12.500	11.000	10.740
Title: Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) ***Description:*** The Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS) program is developing safe and reliable autonomous software agents that can neutralize botnet implants and similar large-scale malware in networked devices. HACCS is developing technologies to (1) identify and characterize botnet-conscripted networks of devices to determine the types of devices and the software services running on them with sufficient precision to infer the presence of known vulnerabilities; (2) generate software exploits for a large number of known vulnerabilities that can be used to establish initial presence in each botnet-conscripted network without disrupting system functionality; and (3) create high-assurance software agents that can autonomously	18.800	15.400	9.240

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
navigate within botnet-conscripted networks, identify botnet implants, and curtail their ability to operate while minimizing side effects to systems and infrastructure. HACCS technologies aim to enable U.S. agencies possessing the appropriate authorities to safely conduct Internet-scale counter-botnet operations. ***FY 2021 Plans:*** - Enhance botnet-tracking algorithms to enable detection and tracking of additional classes of botnet-conscripted networks, such as peer-to-peer (P2P) botnets. - Expand discovery techniques to address additional platforms and classes of software vulnerabilities. - Evaluate botnet-tracking algorithms for detecting botnet-conscripted networks by characterizing botnet management infrastructure, and evaluate autonomous agent behavior in synthetic environments. - Collaborate with transition partners to evaluate counter-botnet technology in synthetic environments. ***FY 2022 Plans:*** - Enhance botnet-tracking algorithms to provide near-real-time assessment for the global identification and tracking of all major classes of botnet-conscripted networks. - Enhance automated discovery techniques to address software vulnerabilities of increased complexity. - Evaluate botnet-tracking algorithms for detecting botnet-conscripted networks by characterizing botnet management infrastructure, and evaluate autonomous agent behavior in real-world environments. - Collaborate with transition partners to select and evaluate counter-botnet technology in realistic environments. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease is the result of reduced counter-botnet technology development and prototype integration work, and focus shifting to demonstrations in collaboration with transition partners.			
Title: Active Social Engineering Defense (ASED) ***Description:*** The Active Social Engineering Defense (ASED) program is developing technologies to automatically identify, disrupt and investigate social engineering attacks via bot-mediated communications. Social engineering attacks, such as phishing and spear-phishing, typically gain user trust via impersonation to induce behaviors or elicit sensitive information that compromise security of an information system. At present, defending against social engineering attacks falls largely to users. ASED aims to prevent social engineering attacks by creating counter-social-engineering bots that act on behalf of users to mediate and aggregate communications and auto-identify attackers. ASED aims to greatly reduce the effectiveness of adversary social engineering attacks and improve the security of DoD information systems. ***FY 2021 Plans:*** - Enhance and refine prototype social engineering attack defense system for use in real-world environments.	12.500	10.800	6.600

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Demonstrate automated attribution of social engineering attacks across multiple communication platforms. - Assess system performance by quantifying the increased costs to an adversary of conducting a social engineering attack. ***FY 2022 Plans:*** - Demonstrate and evaluate a machine-learning-based social engineering attack detection system, including automated attribution of social engineering attacks against advanced simulated adversaries who disguise their attacks. - Harden a modular social engineering attack detection and attribution system for use by U.S. Government, DoD, and industry. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of development of counter-social-engineering bot technologies and focus shifting to demonstration, evaluation and transition to U.S. Government, DoD, and industry.			
Title: Configuration Security ***Description:*** The Configuration Security program is developing technologies to analyze, monitor, and modify the configuration of composed cyber-physical-human systems to identify system vulnerabilities and minimize the attack surface while maintaining functionality and performance. Complex cyber-physical systems, such as ships, airplanes, and critical infrastructure, increasingly make use of multiple commodity information technology components. The manual configuration necessary to enable each component to interoperate introduces exploitable cyber vulnerabilities, as do the standard operating procedures that system operators follow. The Configuration Security program will develop capabilities to automate the appropriate configuration of such systems within the operational context, ensure secure configuration settings, and prevent malicious changes to these settings. ***FY 2021 Plans:*** - Increase automation of best-practice secure configuration generation for operationally relevant, complex cyber-physical-human systems, including the translation of standard operating procedures and figures into machine-understandable formats. - Apply algorithms to automatically reconfigure a civilian critical infrastructure system to a safer and more secure baseline that provides required functionality and supports the new configuration with automatically-generated human-readable explanations. - Test and evaluate a capability to detect and prevent malicious modification of configurations from the system-generated baseline on a shipboard communications system, and to assist system operators in changing between operational contexts. ***FY 2022 Plans:*** - Scale and optimize automatic generation of contextualized secure configurations for operationally relevant, complex cyber-physical-human systems, including the translation of multi-vendor, human-readable artifacts into machine-understandable formats. - Demonstrate algorithms to automatically reconfigure a military operational system to a safer and more secure baseline that provides required functionality and supports the new configuration with automatically-generated human-readable explanations.	14.800	11.400	6.050

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Transition a capability to detect and prevent malicious modification of configurations from the system-generated baseline on multiple DoD-relevant systems, including a shipboard communications system, and to assist system operators in changing between operational contexts. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of algorithm and software development, and focus shifting to demonstrations and transition of an automated capability to detect and prevent malicious modification of configurations for military systems.			
Title: Searchlight ***Description:*** The Searchlight program is developing technologies to ensure that quality-of-service (QoS) guarantees are met for distributed applications operating across the Internet. The increasing use of Internet-based distributed applications creates risks as surges in network use can result in resource shortfalls. Searchlight will develop novel approaches for allocating inherently limited network resources to optimize the performance of distributed applications. Searchlight techniques and systems aim to enable organizations to adapt the QoS for their low-priority traffic resulting in improved QoS for their high-priority traffic without affecting traffic from other Internet users. Searchlight technologies will become increasingly important as 5G systems provide advanced capabilities for organizations to adapt their QoS guarantees. ***FY 2021 Plans:*** - Implement a system that integrates automated application inference, network inference, and QoS management for DoD and commercial networks. - Demonstrate the integrated QoS management system and evaluate its capability on heterogeneous distributed applications of interest to the DoD and commercial network service providers. - Formulate transition approaches with DoD and commercial network service providers. ***FY 2022 Plans:*** - Improve integrated QoS management system performance in terms of scale, application identification accuracy, and application responsiveness. - Demonstrate the integrated QoS management system and evaluate its capability on heterogeneous applications distributed across wide area networks of realistic scale and complexity. - Work with transition partners to optimize the QoS management system to relevant use cases, applications, and network characteristics. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects minor program repricing.	5.300	4.900	4.809
Title: Enhanced Attribution	18.600	8.600	2.750

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
Description: The Enhanced Attribution program is developing technologies to associate the malicious actions of cyber adversaries with individual operators, and to publicly reveal these actions without compromising sources and methods. The program focuses on new approaches for identifying malicious cyber operators, analyzing their software tools and actions, and confirming this information with commercial and public sources of data. As the attribution techniques are developed and show promise, they will provide the basis for new cyber capabilities such as indications and warning of adversary cyber actions. These technologies will be implemented in tools for evaluation by potential transition partners. ***FY 2021 Plans:*** - Integrate additional data sources in the attribution platform, and develop techniques for automated and assisted tasking of defensive capabilities. - Adapt tools and techniques to interoperate with existing software frameworks, and extend capabilities of event extraction techniques. - Work with transition partners to evaluate the attribution platform on new commercial and government-provided data sets, and transition attribution technologies to support operational objectives. ***FY 2022 Plans:*** - Harden the attribution platform and transition to operational partners. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects conclusion of development, integration, and evaluation of the attribution platform, and transition to operational partners.			
Title: Dispersed Computing ***Description:*** The Dispersed Computing program is developing techniques to distribute computing tasks across network computing elements to enable more efficient utilization of enterprise and Internet-based storage, processing, and networking resources. At present, enterprises and Internet-based information technology service providers are increasingly adopting the cloud model, with data storage and computer processing concentrated in large data centers. This brings economies of scale and cost savings to storage and processing, but creates problems for the network and for latency-sensitive applications due to the need to backhaul data to (often distant) data centers for processing. The Dispersed Computing program is developing a dispersed computing architecture that results in more efficient utilization of storage, processing, and networking resources. A key enabler is the recent introduction by vendors of network elements that can be dual-purposed as computational elements. These dual-purpose network-compute elements make it possible to eliminate bottlenecks/chokepoints and to mitigate impossible backhaul requirements by opportunistically moving code to data, given network conditions and available network-compute elements. With	16.300	4.000	2.300

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
Dispersed Computing technology, the network becomes the cloud, and computation is performed where it is most efficient to do so. ***FY 2021 Plans:*** - Increase the operational scale of integrated network-compute elements to thousands of nodes while automatically redistributing workloads. - Optimize and evaluate integrated capabilities over networks with thousands of network-compute elements in terms of the reduction of network bandwidth consumed and the increase in computational utilization. - Demonstrate integrated network-compute capabilities on realistic workloads to Defense Information Systems Agency (DISA) and commercial network providers. ***FY 2022 Plans:*** - Harden and transition integrated network-compute capabilities to DISA and commercial network providers. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects minor program repricing.			
Title: Cyber Assured Systems Engineering (CASE)	15.600	9.780	2.350
Description: The Cyber Assured Systems Engineering (CASE) program is developing the design, analysis and verification tools needed to allow systems engineers to design-in cyber resiliency and manage tradeoffs as they do other quality attributes when designing complex embedded computing systems. The current state of practice for cyber resilience utilizes penetration testing after system construction to drive post-design re-engineering. The CASE technical approach formulates cyber resilience as an explicitly engineered property, similar to other holistic properties such as safety, durability, and reliability now standard in systems engineering. The challenge of resiliency is that it cannot be established through conventional testing methods. CASE will focus on the following technical areas: techniques to derive resilience-related requirements before system design and construction; architectural design and analysis tools to design-in the derived resilience requirements while providing feedback to the human designer to allow for informed tradeoffs between resilience and other system design goals; tools to adapt existing software to support system-level resilience requirements; and inference engines, satisfiability solvers, and provers scalable to complex networked cyber-physical systems. CASE technologies will enable the design of cyber-physical systems that robustly execute their intended function despite the efforts of sophisticated cyber adversaries. ***FY 2021 Plans:*** - Enhance cyber resilience design tools based on the results of integrating into the engineering workflow of a defense system provider. - Evaluate and demonstrate design tools and techniques on defense platforms including a military helicopter.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Demonstrate the ability of a defense platform provider to use design tools to produce cyber resilient designs. - Demonstrate enhanced platform cyber resiliency in tests coordinated with potential transition partners and other stakeholders. ***FY 2022 Plans:*** - Harden technologies for cyber security systems engineering and transition to DoD stakeholders for demonstration and evaluation in programs of record. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects ramping down of development and demonstration of techniques and software tools to design-in cyber resiliency requirements, and transition of capabilities to programs of record.			
Title: Open, Programmable, Secure 5G (OPS-5G) ***Description:*** The Open, Programmable, Secure 5G (OPS-5G) program, addressing key technical issues explored in the Searchlight program (also budgeted in this PE and Project), will develop open source, 5G network software that ensures security and stimulates innovation in mobile wireless hardware. Current trends in mobile wireless technology development are unfavorable in that the U.S. 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 of transparent, open source technology created by a diverse ecosystem of academic and commercial software and hardware developers. OPS-5G will be coordinated with existing open-source 5G efforts and U.S. Government, DoD, and industry stakeholders. ***FY 2021 Plans:*** - Formulate approaches for addressing 5G security challenges, such as eavesdropping at access points and denial of service. - Formulate approaches for automatically extracting information relevant to software implementations including software structure, service interfaces, timing parameters, flow diagrams, and protocol graphs from 5G standards maintained in electronic documents. - Formulate 5G node and network security architectures, and initiate development of tools for integrity checks, attack prevention, remote diagnosis and service recovery. - Devise in-network sensors and reactive defenses for attack onset detection and scalable resilience against distributed denial of service (DDoS) attacks in 5G networks. ***FY 2022 Plans:*** - Implement and evaluate prototype systems that address 5G security challenges, such as eavesdropping at access points and denial of service.	-	11.800	21.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Implement and evaluate prototype software for automatically extracting information relevant to software implementations including software structure, service interfaces, timing parameters, flow diagrams, and protocol graphs from 5G standards maintained in electronic documents. - Implement and evaluate 5G node and network security technologies and tools for integrity checks, attack prevention, remote diagnosis, and service recovery. - Assess and develop information protection techniques suitable for current and future mobile wireless systems to support DoD operational security needs. - Demonstrate prototype systems to commercial vendors, commercial service providers, the DoD, and other U.S. Government stakeholders. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects ramping up of development and implementation of 5G network security technologies, and initial demonstration and evaluation in collaboration with open-source 5G efforts and U.S. Government, DoD, and industry stakeholders.			
Title: Program Analysis for Capability Excellence (PACE)*	-	10.400	19.250
Description: *Formerly Cyber Course of Action Analysis (C2A2) The Program Analysis for Capability Excellence (PACE) program will develop tools and techniques to autonomously identify adversary compromise of software, mitigate negative effects of adversary capabilities, and restore the integrity of compromised software. PACE will enable rapid, autonomous response to cyber attacks without using source code or requiring recompilation. ***FY 2021 Plans:*** - Develop techniques for autonomously characterizing and identifying software under attack via emergent computation. - Develop attack-specific mitigations that can be rapidly generated and deployed with minimal human assistance. ***FY 2022 Plans:*** - Implement emerging software compromise identification and mitigation techniques in an initial proof-of-concept autonomous system. - Demonstrate techniques for attack-specific mitigations that can be rapidly generated and deployed with minimal human assistance. - Assess autonomous system performance against synthetic attacks representative of real world threats. ***FY 2021 to FY 2022 Increase/Decrease Statement:***			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
The FY 2022 increase reflects continued development of techniques for autonomously identifying and mitigating compromise and expanded efforts related to implementation and assessment.			
Title: Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)	-	9.800	14.750
Description: The Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS) program, addressing issues encountered in the Cyber Assured Systems Engineering (CASE) program, budgeted within this PE and Project, will create 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 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, replacing legacy software components with technologically superior ones for improved performance or security faces high risk that the new software, despite being proven correct according to a specification, 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 technology will iteratively and interactively leverage automated program understanding to semi-automatically derive a DSL for the targeted component of a large code base, translate the code for the component into this DSL while concurrently inferring its specification within the larger environment, and then generate, optimize, and distribute executable artifacts across the system, creating and validating relevant proofs. V-SPELLS aims to enable piecewise, compatible-by-construction improvement of software components in legacy DoD systems, providing to incremental software (re)engineering the benefits of formal software verification currently available only to clean-slate development efforts. ***FY 2021 Plans:*** - Formulate automated techniques for decomposing legacy code into functional modules with domain data structure and operation definitions. - Design a development environment for convergent DSL programming, including compatibility-centric program analysis techniques. - Explore alternative compilation techniques for DSL virtual machine stacks that are tunable for performance, security, diversity, and verifiability. ***FY 2022 Plans:*** - Implement automated techniques for decomposing legacy code into functional modules with domain data structure and operation definitions, untangling of legacy code into low-level domain operation implementations and higher-level application logic, and lifting of legacy code into an extracted DSL.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Create an initial development environment for convergent DSL programming, including compatibility-centric program analysis techniques that provide efficient, intelligible feedback and refined counterexamples to developers. - Identify DoD software environments that would benefit from recoding selected legacy components using DSLs for packet filtering, data, signal, and image processing, and other latency-sensitive/security-critical functions. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects ramping up of work to develop automated techniques for decomposing legacy code into functional modules, compilation techniques for DSL virtual machine stacks, and an initial development environment.			
Title: Hardware Optimization (HOP) ***Description:*** The Hardware Optimization (HOP) program, addressing technical issues encountered in the Rapid Attack Detection, Isolation and Characterization Systems program, also budgeted within this PE and Project, seeks to develop hardware optimizations for national security purposes. Specifically, HOP will enable new national security workloads in high performance microelectronic hardware. This research will produce end-to-end hardware optimization toolkits to enhance hardware designs. These toolkits will be comprised of algorithms, digital design files, documentation, and binaries. ***FY 2021 Plans:*** - Identify and establish a wide area network (WAN) to support program research and transition efforts. - Begin development of design specifications, architectures, and fabrication. ***FY 2022 Plans:*** - Evaluate hardware optimizations to address algorithmic improvements and address scalability and performance opportunities. - Design and develop initial alternative implementations for hardware optimizations. - Provide initial hardware optimizations to an evaluator for performance assessments and evaluations. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects ramping up of work to develop alternative implementations for hardware optimizations.	-	6.100	13.100
Title: Bio Cyber Security (BCS) ***Description:*** The Bio Cyber Security (BCS) program aims to develop technologies to address the large attack surface of automated experimental bio-cyber-physical laboratories. As biology becomes increasingly an information-driven discipline, and biological experimentation becomes increasingly automated, the attack surface of the integrated bio-cyber-physical infrastructure that enables modern biotech is expanding. The BCS program will use big data technologies, artificial intelligence (AI), machine learning (ML), and advanced bio-informatics to create automated surveillance and defense algorithms that can detect and respond in real-time to high-speed, coordinated attacks on bio-cyber-physical laboratories. The BCS program aims to develop technologies	-	-	6.600

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
to assure the U.S. biotech enterprise and to thwart attempts to compromise the availability, integrity, or safety of U.S. biotech infrastructure. ***FY 2022 Plans:*** - Introduce and refine methods for capturing, organizing, and understanding the information flows, control signaling, and potential vulnerabilities within a bio-cyber-physical laboratory. - Formulate big data, AI, and ML-based approaches for detecting anomalies in the sense-process-actuate loops inherent to automated biotech experimentation. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects program initiation.			
Title: Rapid Attack Detection, Isolation and Characterization Systems (RADICS) ***Description:*** The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is developing automated systems to enable a black start recovery of the U.S. power grid amidst a cyber attack on the energy sector's critical infrastructure. The RADICS program aims to enable skilled cyber and power engineers to rapidly restore electrical service after an attack that challenges the recovery capabilities of the impacted organizations (e.g., utilities, balancing authorities, independent system operators, bulk power markets). The potential for a cyber-enabled attack on the U.S. power grid is a national security issue, as the ability of the military to deploy and project force is dependent on the effective and efficient functioning of civilian logistics and supply systems. The program will develop technologies to monitor heterogeneous distributed networks, detect anomalies that require rapid assessment, isolate compromised system elements, establish secure emergency communications networks, characterize attacks, and detect sensor spoofing. The technology development is coordinated with and will transition to U.S. Government elements responsible for the defense of critical infrastructure. ***FY 2021 Plans:*** - Test inoperability of a utility to utility radio communication network that would facilitate integration and coordination among independent and disparate organizations in a large-scale trans-regional black start scenario. - Collaborate with private industry, DOE, DHS, DoD, and other stakeholders to demonstrate enhanced capabilities for black start restoration of a power grid amidst a cyber-attack. - Harden and transition technology and capabilities to U.S. Government, National Guard, and industry. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects program completion.	20.350	3.177	-
Title: Leveraging the Analog Domain for Security (LADS)	10.981	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
Description: The Leveraging the Analog Domain for Security (LADS) program developed techniques for defending information systems by advantageously using side channel signals such as radio frequency and acoustic emissions, power consumption, heat generation, differential fault analysis, and timing-based effects. LADS augments standard cybersecurity approaches, which focus on digital effects, with analog techniques. LADS technologies can enable defenders to detect cyber attacks by sensing changes in the analog emissions of computing components, devices, and systems, greatly complicating the task of adversaries who wish to remain hidden.			
Title: Brandeis ***Description:*** The Brandeis program created the capability to dynamically, flexibly, and securely share information while ensuring that private data may be used only for its intended purpose and no other. Brandeis technologies can resolve the tension between maintaining privacy and being able to tap into the huge value of data. In the civilian sphere, there is a recognized need for technologies that enable the controlled sharing of information between commercial entities and U.S. Government agencies. Similarly, the U.S. military is increasingly involved in operations that require highly selective sharing of data with a heterogeneous mix of allies, coalition partners, and other stakeholders. Brandeis technologies are designed to work with the virtualization, cloud computing, and software-defined networking technologies now widely used in both civilian and military environments.	6.620	-	-
Title: Extreme Distributed Denial of Service Defense (XD3) ***Description:*** The Extreme Distributed Denial of Service Defense (XD3) program developed new computer networking architectures that deter, detect, and overcome distributed denial of service (DDoS) attacks. DDoS attacks include both high-volume flooding attacks and more subtle low-volume attacks that evade traditional intrusion detection systems while exhausting server processing and memory. These attacks will accelerate as the Internet of Things (IoT) incorporates new classes of devices that in many cases will be deployed with inadequate security controls: attackers will conscript poorly defended IoT devices into their botnets. XD3 developed defensive architectures that use maneuver, deception, dispersion, and on-host adaptation to increase adversary work factors, boost resilience of mission critical services such as command and control, and thwart DDoS attacks.	5.750	-	-
Accomplishments/Planned Programs Subtotals	261.861	236.182	237.089

	FY 2020	FY 2021
Congressional Add: Distributed Ledger Technology ***FY 2020 Accomplishments:*** - Conducted research in Distributed Ledger Technology.	1.000	-
Congressional Adds Subtotals	1.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**Project (Number/Name)** IT-03 / *CYBER SECURITY*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
IT-04: *ARTIFICIAL INTELLIGENCE AND HUMAN-MACHINE SYMBIOSIS*	-	139.824	178.162	193.274	-	193.274	-	-	-	-	-	-

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 trusted partners to human operators. Of particular interest are systems that can understand human language and extract information and reliably categorize content contained in diverse media; answer questions, reach conclusions, and propose explanations; and learn, reason, and apply knowledge gained through experience to respond intelligently to new and unforeseen events. Enabling computing systems with such human-like intelligence is now of critical importance because the tempo of military operations in emerging domains exceeds that at which unaided humans can orient, understand, and act. The technologies developed in the Artificial Intelligence and Human-Machine Symbiosis project will enable warfighters to make better decisions in complex, time-critical, battlefield environments; intelligence analysts to make sense of massive, incomplete, and contradictory information; software developers and certifiers to design, implement, evaluate, and accredit cyber-physical systems and other complex software-reliant systems with greater efficiency and confidence; and unmanned systems and semi-autonomous agents to perform critical missions in contested physical and virtual environments safely and reliably. This Project includes FY 2020 CARES Act funding in the amount of $.619 million to apply artificial intelligence (AI)-based models to rapidly screen, prioritize and test Food and Drug Administration (FDA)-approved therapeutics for new COVID-19 drug candidates.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Accelerating Artificial Intelligence (AAI)	44.575	40.820	35.100
Description: The Accelerating Artificial Intelligence (AAI) program seeks to go beyond commercially-driven advances in AI and to address important national security challenge applications. In particular, this program is focused on improving human-AI collaborations to mitigate current bottlenecks in DoD's ability to rapidly adapt and deploy new technologies and capabilities. If successful, research efforts under this program will significantly accelerate the pace of innovation in many important DoD domains while also reducing the time and cost associated with approval and certification processes needed to transition and deploy new technologies. One technical challenge to be addressed in this program is the need to assess current developmental, approval, and certification processes and identify tasks or sub-tasks amenable to greater automation with minimal human intervention. Other challenges include the need to develop social context aware AI systems and to ensure robustness of AI systems, particularly in novel and/or unanticipated situations. Approaches to addressing these challenges will leverage recent advances at the frontiers of AI research in transfer learning, causal reasoning and associated models. AAI application areas include the following: (1) machine-enabled techniques to efficiently capture, generate, and analyze disparate data sources to accelerate design and development of new materials and chemistries for DoD specific applications; and (2) knowledge management tools that can efficiently capture and disseminate an organization's expertise, experience and data; and (3) social context informed			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
AI approaches to enable reliable and robust forecasting and decision aiding tools for stabilization, deterrence and gray zone operations. ***FY 2021 Plans:*** - Select military application(s) into which to insert and evaluate novelty-aware AI technologies. - Initiate transition of novelty generation technologies from research domains to military application domains. - Evaluate potential for novelty generators and novelty-robust AI techniques in military application domains to rapidly identify and respond appropriately to new classes, attributes, relationships, representations, capabilities, and interactions. - Validate process and property optimization capabilities of molecular design systems through challenges informed by DoD applications. - Develop new time-aware neural network architectures that introduce meta-learning capabilities for time cognition in machine learning. - Implement a reconfigurable kernel toolkit for application development in either a communications or radar based suite to achieve 10x improvement in the system performance of input signal-to-noise sensitivity or signal-to-interference rejection ratio. - Create a comprehensive, automated software framework that can take in a microelectronic system design, train effective machine learning surrogate models of sub-system components and integrate them back into the original design to achieve significant simulation speed-ups while maintaining acceptable levels of accuracy and coverage. - Ingest written doctrine and develop a set of rules and algorithms for adversary brigade offensive operations. - Perform initial demonstrations of artificial intelligence algorithms against a live adversary. - Demonstrate relative effectiveness, extensibility of methodologies for creating empirical measures of game balance state equations. - Demonstrate methodology for effective identification, introduction, and quantification of game/model modifications that create significant imbalance. - Develop and demonstrate automated analysis of electrical and mechanical computer aided design (CAD) documentation datasets to identify notable features and export them in graphs and a human-readable summary format for analysts. - Develop techniques to automatically discover the minimal features needed to distinguish between the members of sets of objects and actions. - Conduct a comprehensive survey of current state-of-the-art in neural net-based computer vision systems, adversarial attack methods and approaches, defenses against adversarial attack methods and approaches, and current research directions in all of the above. - Develop universal attack algorithms that cause misclassification of a single object class. - Demonstrate performance on at least three different deep neural networks. - Begin real-time, in vivo evaluation of AI-enabled neural interface architectures.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Continue efforts to accelerate Artificial Intelligence with a focus on third wave AI. ***FY 2022 Plans:*** - Extend evaluation of novelty generators and novelty-robust AI techniques in military application domains to include new environments, goals, and context. - Initiate transition of molecular design systems from academia and industry to DoD partners for evaluation in DoD applications. - Define and validate parameters for inverse design of molecules with relevance to DoD applications. - Prototype time-aware meta-learning methods and demonstrate novel machine intelligence capabilities. - Initiate efforts to improve human operators' ability to innovate with their AI-enabled platforms. - Explore opportunities for rapid development and test environments for designing interfaces that improve human operation of AI-enabled platforms. - Explore automated approaches for managing language and knowledge encountered in specialized domains, extracting the essential facts in a stream of inputs, and translating between domain-specialized representations and common English. - Describe the technical approach for 1) intelligent array operations, 2) application development in a tensor-based programmable language, and 3) hardware implementation. - Develop a model that demonstrates the combined array and machine learning (ML) algorithms and how the intelligent array algorithms are abstracted to hardware-independent operations. Report on use cases descriptions of the new array-ML architecture. - Develop techniques to automatically discover the new features needed to accommodate differences between newly acquired objects and actions and those previously learned. - Continue efforts to accelerate Artificial Intelligence with a focus on third wave AI. - Quantify competency-aware capabilities with relevance to DoD applications. - Identify DoD experimental platforms and partners to demonstrate competency-aware capabilities. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects a shift from development and prototyping to testing.			
Title: Symbiotic Design ***Description:*** The Symbiotic Design program is developing artificial intelligence-based approaches to augment human teams in the design of cyber-physical systems (CPS), and thereby significantly reducing time to deployment and improving the quality of deployed systems. The current generation of DoD systems and platforms integrate cyber and physical subsystems, but the capability of the engineering teams has not scaled with the enormous complexity of modern CPS. Engineering organizations require large teams of engineers that collectively possess the necessary domain knowledge (of component technologies, theories, and tools), but the prolonged timelines of the development process for modern CPS hinders DoD's ability to counter emerging threats. The Symbiotic Design program will address the challenge by transforming the human-focused, model-based design flows	12.809	25.582	28.100

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
used today into a symbiotic process of collaborative analysis by humans and continuously-learning AI-based co-designers. The program will create technologies essential for AI co-design: design space construction, design composition, and design space exploration. The program will demonstrate the approach at realistic scales by a sequence of CPS design challenges of increasing complexity, and quantify the results with respect to development time, system performance, quality, and innovation metrics. ***FY 2021 Plans:*** - Create techniques for defining design spaces and for evaluating design points using domain-specific analysis and simulation tools. - Develop prototype design mining engines and feature extractors to enable query generation from seed designs and to extract heterogeneous model-based design artifacts. - Develop techniques for exploring high-dimensional, multi-domain, combinatorial design spaces and design elaboration methods for automated model completion by an AI co-designer across multiple design domains. ***FY 2022 Plans:*** - Expand scope and domain coverage of design mining engines to allow incremental construction of design spaces. - Develop cross-domain inferencing techniques to automate cross domain reasoning and model learning. - Develop prototype tools to accelerate high fidelity model analysis and simulation, visualize and understand high dimensional design spaces, and shape and guide design exploration. - Produce design challenge problems related to sub-systems and systems of interest to the DoD, and evaluate the effectiveness of symbiotic design technologies. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects continued development and implementation of symbiotic design techniques and expanded evaluation on systems of interest to DoD.			
Title: Automated Rapid Certification Of Software (ARCOS) ***Description:*** The Automated Rapid Certification Of Software (ARCOS) program is developing technologies that automate the evaluation of software assurance evidence to enable certifiers to assess system risks earlier in the process and more rapidly and safely commit to engineering decisions. 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.	16.100	28.860	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2021 Plans: - Extend assurance-case engineering tools to facilitate the design and implementation of software and associated assurance evidence. - Develop approaches to analyze legacy software assurance evidence and specifications to determine areas of insufficient assurance. - Scale data structure representations to accommodate assurance evidence from complex military platforms such as a military helicopter. - Demonstrate and validate automatically-generated assurance case arguments. ***FY 2022 Plans:*** - Develop approaches to augment assurance evidence for legacy software to provide stronger fitness arguments. - Demonstrate automatically calculated confidence measures for assurance case arguments that are objectively meaningful. - Demonstrate the composability of automatically generated assurance case arguments to support incremental evaluations. - Reduce the computation time necessary to automatically generate assurance case arguments for complex military platforms such as a military helicopter. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects a shift from development of assurance case engineering techniques and tools to demonstration of techniques on representative military platforms.			
Title: Knowledge-directed Artificial Intelligence Reasoning Over Schemas (KAIROS)	13.000	21.100	19.000
Description: The Knowledge-directed Artificial Intelligence (AI) Reasoning Over Schemas (KAIROS) program is developing AI and machine learning technologies to aid a human operator in understanding complex sequences of events in the world. For the purposes of KAIROS, an event is an occurrence that results in an observable and recognizable change in either the physical world or human activity. Events of particular interest to KAIROS are those that create changes that have significant impact on national or homeland security. The KAIROS program will develop automated systems that codify existing event-representation schemas and, when needed, create and codify new schemas to bring structure to complex event sequences and present these structured representations to operators. Given multi-media inputs, operators will use KAIROS technologies to identify subsidiary event elements, determine their temporal order, recognize complex event sequences, and link disparate events. KAIROS technologies aim to enable analysts and warfighters to understand unfolding events rapidly and accurately. ***FY 2021 Plans:*** - Develop and assess the capability for machine learning of complex schemas from large multimedia data sets. - Develop and evaluate the capability for matching unfiltered simple events from unconstrained large data sets to an initial schema library.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Develop and assess machine learning classifiers for categorizing the temporal and causal relationship between two simple events that are part of a complex event sequence. - Collaborate with transition partners to establish thresholds for mission utility for anticipating future events that are part of partially-observed complex events in operational data. ***FY 2022 Plans:*** - Develop capability for machine learning of the similarities and differences in the structural features of various complex event schemas. - Develop the means to curate the schema library and methods for identifying intermediate levels in the structure of the library. - Develop a user interface to probe input sources for missing information and to provide interactive feedback. - Collaborate with transition partners to evaluate systems on complex real-world event sequences and identify necessary adjustments. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects the shift from development of techniques for learning complex schemas to assessment of techniques on operational data.			
Title: Active Interpretation of Disparate Alternatives (AIDA)	14.790	22.300	16.950
Description: The Active Interpretation of Disparate Alternatives (AIDA) program is developing a multi-hypothesis semantic engine that generates alternative interpretations of events, situations, and trends from a variety of unstructured sources where there are noisy, conflicting, and potentially deceptive data. At present, information from each medium is often analyzed independently, without the context provided by information from other media, with only informal comparison among competing hypotheses. The consequence of this can be inadequate interpretations, because alternatives are eliminated due to lack of evidence even in the absence of contradictory evidence. AIDA seeks to develop and demonstrate technology to automatically map information derived from diverse media into a common semantic representation, aggregate information, resolve ambiguities, discover conflicting information, and generate and explore multiple interpretations of events, situations, and trends. AIDA aims to provide decision makers a capability to understand alternative explanations for available information and to make contingency plans accordingly. ***FY 2021 Plans:*** - Develop the means to rank hypotheses according to relevance and confidence, and the capability to verify and explore hypotheses developed by users. - Enhance the capability of the system to infer components of hypotheses not explicit in the input. - Enhance the interface to facilitate the capability of the user to refine the extracted semantic elements and the generated hypotheses.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Collaborate with transition partners to conduct experiments to evaluate performance on operational data. ***FY 2022 Plans:*** - Develop the means to detect seemingly minor but important changes in otherwise similar documents to enable discovery and analysis of different hypotheses. - Develop the means to change statistical priors for new sources to reflect known biases and reliability, and thereby enable more accurate computation of coherence measures. - Enhance interface capabilities to facilitate exploration of user-generated conjectures and other models of human-computer interaction. - Collaborate with transition partners to conduct experiments to evaluate extraction and hypothesis generation performance on operational data. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects the shift from development of techniques for generating multiple alternative interpretations from multimedia data to evaluations of techniques on real-world data.			
Title: Assured Autonomy	16.000	15.000	13.000
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 2021 Plans:*** - Integrate learning-enabled components with examples of formally verified safety properties into autonomous systems, and implement scalable algorithms for dynamic evaluation of assurance cases. - Develop and evaluate scalable monitoring techniques to detect data-distribution shifts on simulated and real-world data in which the operating environment diverges from the training environment.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Develop scalable techniques for runtime verification of learning-enabled systems, and integrate safety constraints in online learning algorithms to allow safe operation of autonomous systems in proximity to humans in unknown and unstructured environments. ***FY 2022 Plans:*** - Evaluate the impact of safety-constraints incorporated in online learning algorithms on the performance of autonomous systems operating in unknown and unstructured environments. - Demonstrate technologies on assurance challenge problems for several learning-enabled autonomous platforms of interest to the DoD. - Perform improvements to formal verification tools and monitoring techniques, and transition technologies to industry and DoD. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects the shift from development efforts to demonstrations on several learning-enabled autonomous platforms, and transition to industry and DoD.			
Title: Explainable Artificial Intelligence (XAI)	18.550	17.200	9.324
Description: The Explainable Artificial Intelligence (XAI) program is developing a new generation of machine learning techniques that are able to explain their rationale, characterize their strengths and weaknesses, and convey an understanding of how they will behave in the future. AI is a critical enabler for U.S. military systems that will perform increasingly complex and sensitive missions. However, in order for developers, users, and senior leaders to feel confident enough to deploy and use AI-enabled systems, these systems must be able to explain their rationale, and their recommendations, decisions, and actions must be delivered in a way that military users can understand and trust. Today, most machine learning systems provide no explanations, or provide explanations that are at the wrong level of abstraction, not meaningful to a human user, or inconsistent with the full range of behaviors of the AI system. XAI is developing the tools necessary to build explainable AI systems, specifically with: (1) new machine learning techniques that produce human-interpretable models and (2) user interfaces that generate explanations from those models that are meaningful to end-users, using natural language, saliency maps, and other representations. XAI implementations will be developed and demonstrated in next-generation data analytics and autonomous systems. ***FY 2021 Plans:*** - Enhance explainable systems for robustness to increased machine learning task complexity. - Expand the cognitive model of explanation based on task performance evaluations. - Measure system explainability, accuracy, and learning performance against additional datasets and scenarios. - Select and integrate subsets of explainable model techniques in prototype systems for capability demonstrations coordinated with DoD and Intelligence Community (IC) partners. ***FY 2022 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Refine the cognitive model of explanation based on the results of prototype system capability demonstrations. - Optimize integrated explainable AI prototypes and quantify system explainability, accuracy, and learning performance against additional datasets and scenarios in capability demonstrations coordinated with DoD and IC partners. - Create an explainable AI toolkit, and transition datasets and code. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 decrease reflects the shift from development and integration of explainable machine learning techniques and systems to testing, performance assessment, and transition.			
Title: Engineering Artificial Intelligence Systems Implementations (EAISI) ***Description:*** The Engineering Artificial Intelligence Systems Implementations (EAISI) program will create technologies and tools to support the development of viable and trusted systems that include AI and machine learning (ML) capabilities. Modern AI-dependent systems may include multiple AI components, drawing on a diverse set of AI-related techniques, ranging from ML to knowledge representation, search, planning, game theory, and optimization. Current methods for development of such systems remains primarily based on trial-and-error designs, with limited abstractions, architectures, and patterns. These developments can be costly, risky, and demanding of very high levels of expertise. To address this, EAISI will develop abstractions, patterns, architectures, assurance techniques, and iterative processes that facilitate the analysis and synthesis of complex systems that must rely on AI-based components and associated training data. One of the more difficult engineering challenges with AI is evaluation and assurance, since AI-based systems tend to resist traditional approaches to testing, inspection, and analysis. It is not possible to fully test an AI-based system for every situation it will ever encounter, so new techniques are needed for verifying and validating AI-based systems. EAISI aims to create software and systems engineering techniques, tools, and practices to facilitate the development of AI-based systems that are capable, trustworthy, affordable, and timely. ***FY 2021 Plans:*** - Formulate rigorous approaches for managing training data for AI-based systems, including provenance, security, and quality in the engineering of an AI-based system. - Devise approaches for testing, analyzing, and evaluating AI-based systems as means for gaining confidence in and validating those systems. ***FY 2022 Plans:*** - Develop prototype tools for managing training data for AI-based systems, including provenance, security, and quality in the engineering of an AI-based system. - Develop prototype tools for testing, analyzing, and evaluating AI-based systems including intuitive visualization techniques that give users a realistic understanding of the confidence that is warranted when validating those systems.	-	7.300	9.800

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Devise a framework and associated interfaces for integrating prototype tools in an AI systems engineering development environment for use by developers and evaluators who are not experts in AI. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects ramping up of the development of AI systems engineering technologies and their integration in an AI systems engineering development environment for use by developers and evaluators who are not experts in AI.			
Title: Counter Adversarial Artificial Intelligence ***Description:*** The Counter Adversarial Artificial Intelligence program aims to enhance the capability to detect, deflect, and diminish the effects of adversarial attacks on AI-based systems. Defense systems increasingly incorporate artificial intelligence (AI) capabilities such as machine learning and automated reasoning. These AI-enabled systems are typically engineered and optimized for environments where adversary systems are either static or strictly limited in terms of adaptive behaviors. Engagements between sophisticated AI-enabled systems are likely to become increasingly common going forward. Maintaining AI-superiority for the U.S. will require systems with higher levels of capability. Specific capabilities to be developed include recognizing when an adversary system is AI-enabled, identifying and modeling adversary AI capabilities based on empirical data, and creating counter-AI strategies including techniques to render adversary AI capabilities ineffective and/or deleterious. ***FY 2022 Plans:*** - Begin modeling the range of potential adversarial AI behaviors, including the nature of vulnerabilities in machine learning components and symbolic AI components. - Conceptualize AI systems with capabilities to detect, deflect, and diminish the effects of adversarial attacks. - Formulate approaches for recognizing when an adversary system is AI-enabled, identifying and modeling adversary AI capabilities based on empirical data, and countering adversary AI strategies including techniques to render AI capabilities ineffective and/or deleterious. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects program initiation.	-	-	12.000
Title: Artificial Intelligence Reliability and Traceability (AIRT) ***Description:*** The Artificial Intelligence Reliability and Traceability (AIRT) program will develop design-time and run-time technologies to ensure the correct functioning of AI-enabled systems. As AI deployment scales up, it becomes more important for machine learning (ML) systems to be explainable, which means providing rationale for classifications, characterizing confidence level of the classifications, and, as a consequence, conveying understanding of how the system will behave with similar inputs. Explainability, however, is not sufficient to ensure that ML systems meet reliability requirements, in the sense that the ML operates consistently with domain-focused predictive models, nor traceable, in the sense that there are mappings between the models and	-	-	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
the ML behaviors. AIRT will develop the test, evaluation, verification, and validation (TEVV) technologies that system developers need to ensure that AI-enabled systems will correctly perform their intended functions. The AIRT TEVV technologies will address the challenge of how to specify AI-related behaviors and then how to verify the specified behaviors using both analytic formal approaches, which emphasize mathematical modeling and reasoning, and traditional statistical-sampling based approaches. AIRT will also develop design principles for machine learning and related systems that enhance reliability and traceability without appreciable compromise to reasoning capability. Additionally, AIRT will develop traceability approaches that model the learning behavior of an AI component to enable developers, testers, and operators to gain detailed knowledge of how the AI system reached a computational state. The AIRT program aims to make the design and operation of AI systems more scientific and safe. ***FY 2022 Plans:*** - Formulate approaches for TEVV of AI-enabled systems to increase confidence in correct performance of intended functions. - Explore TEVV approaches that include means to specify intended AI-related behaviors and that combine analytic formal approaches, which emphasize mathematical modeling and reasoning, with traditional statistical-sampling based approaches. - Introduce traceability approaches akin to check-pointing and other roll-back techniques that can enhance knowledge of how an AI system reached a computational state. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects program initiation.			
Title: Control System Introspection ***Description:*** The Control System Introspection program seeks to develop machine introspection and learning technologies to characterize a damaged or modified military platform from its behavior, and update the control law to maintain stability and control. A platform equipped with Control System Introspection technologies will continually compare the real-time behavior of the platform as measured by on-board sensors with a learned model, determine if the current observed behavior of the platform differs from that model in ways that might compromise stability and control, and implement an updated control law when required. The current approach to handling platform damage or modification places the burden of recovery and control on the operator, whether the operator is human or an autonomous controller. In contrast, the Control System Introspection capability would aid operators in maintaining effective control of military platforms that suffer damage in battle or have been modified in the field to address emergent requirements identified during operations. ***FY 2022 Plans:*** - Explore machine introspection and learning approaches for identifying the behavioral characteristics of a platform in terms of the transfer function and related control-theoretic models in real time. - Architect machine introspection and learning algorithms that can run in the background on platforms for which the available computational resources are limited.	-	-	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Defense Advanced Research Projects Agency		Date: May 2021
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 2020	FY 2021	FY 2022
- Design and implement an operator-in-the-loop testbed for assessing integrated machine introspection and learning approaches for recovery and control of military platforms that suffer damage in battle or are modified in the field. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The FY 2022 increase reflects program initiation.			
Title: Low Resource Languages for Emergent Incidents (LORELEI) ***Description:*** The Low Resource Languages for Emergent Incidents (LORELEI) program developed technology to rapidly field machine translation and other language processing capabilities for low-resource foreign languages. The U.S. military operates globally, and frequently encounters low-resource languages, which are languages for which few linguists are available and automated human language technologies do not exist. Processing foreign language materials requires protracted effort, and current systems rely on huge, manually-translated, manually-transcribed, or manually-annotated data sets. As a result, systems currently exist only for languages in widespread use and in high demand. LORELEI took a different approach by leveraging language-universal resources, projecting from related-language resources, and fully exploiting a broad range of language-specific resources. The resulting capabilities can rapidly provide situational awareness based on information from low resource languages encountered during emergent missions such as humanitarian assistance/disaster relief, terrorist attack response, peacekeeping, and infectious disease response.	4.000	-	-
Accomplishments/Planned Programs Subtotals	139.824	178.162	193.274

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A