Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Office of the Secretary Of Defense	Date: May 2021
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*

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	-	24.454	25.245	15.380	-	15.380	-	-	-	-	-	-
003: *Cyber Applied Research*	-	24.454	25.245	15.380	-	15.380	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

The Cyber Security Applied Research program element promotes innovative higher risk cyber research to address joint force challenges in full spectrum cyber operations. The program addresses joint Service science and technology (S&T) gaps that influence DoD cyber research priorities and shapes the direction of the wider cyber community. The program integrates both defensive and offensive cyber research to develop interchangeable, defense-wide technology options to meet Combatant Command (CCMD) needs and requirements. To better align itself to the National Defense Strategy (NDS), Department of Defense (DoD) Cyber Strategy, and Office of Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Modernization - Road to Dominance cyber initiative, the program recalibrated research thrust areas to pivot towards emphasizing a need for power projection and taking the fight to the adversary. The established research thrusts areas are: Behavior Cyber Science, Self-Securing Systems, Precise Cyber Effects, and Applied Mathematics for Cyber.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	25.118	15.255	15.586	-	15.586
Current President's Budget	24.454	25.245	15.380	-	15.380
Total Adjustments	-0.664	9.990	-0.206	-	-0.206
• Congressional General Reductions	-	-0.010			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	10.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.660	-			
• Program Adjustment	-	-	-0.206	-	-0.206
• Cancelled Account	-0.004	-	-	-	-

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2020	FY 2021
Project: 003: *Cyber Applied Research*		
Congressional Add: *Cyber Institutes at Institutions of Higher Learning*	10.000	10.000
Congressional Add Subtotals for Project: 003	10.000	10.000
Congressional Add Totals for all Projects	10.000	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense			Date: May 2021
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602668D8Z / *Cyber Security Research*	Project (Number/Name) 003 / *Cyber Applied Research*	

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
003: *Cyber Applied Research*	-	24.454	25.245	15.380	-	15.380	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

Adversaries are increasingly leveling the cyber playing field by harnessing commoditized and affordable cyber tools and capabilities, while developing sophisticated and automated technologies and tactics. The DoD cyber S&T community must accelerate the pace of innovative research accordingly to maintain technological advantage. The 2018 National Defense Strategy (NDS) recognized cyber as an actively contested domain with significant security challenges and potential leap-ahead capabilities for military operations. This was further reinforced by the establishment of Cyber as one of USD(R&E) Modernization Areas in 2018 and development of the USD(R&E) S&T Strategy for Cyber.

This cybersecurity program element focuses on higher risk research ideas with major potential impact for addressing NDS and Modernization mission focus areas of cybersecurity. The program works to advance the state of cybersecurity by reducing risk, broadening applicability, and accelerating research in the areas of Behavioral Cyber Science; Self-Securing Systems; Precise Cyber Effects; and Applied Mathematics for Cyber. Advances in these cyber S&T thrusts will promote strong foundations, while disruptive innovations will create surprise, shape the fight, and ensure a decisive advantage. The thrusts are critical to the development of innovative and sustainable research that takes cybersecurity beyond the incremental escalation of attack and defense. The thrusts provide an opportunity to identify and advance foundational technologies to support all Services and Agencies.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: OUSD (R&E) Cyber Technologies	14.454	15.245	15.380
Description: Integrating both defensive and offensive innovative cyber research within the DoD cyber science and technology (S&T) enterprise to develop interoperable, defense-wide technology options that address joint force challenges in full spectrum cyber operations. Research in Behavioral Cyber Science: Advances understanding and technical rigor of modeling and predicting human responses to cyber activities that enhance cyber operations through planning and training. Explores the interaction between computers and human behavior, moving beyond electronic signals (ones and zeroes) to enable development of new insights to human behavior. Self-Securing Systems: System, platforms, and networks will autonomously help DoD operators react more quickly to cyber-attacks. Equips future DoD systems with the capability to proactively, autonomously, and seamlessly access cyber threats and deploy self-securing mechanisms to neutralize cyber-attacks, offers blue force an innovative new disruptive capability. Precise Cyber Effects: Provides scalable cyber options for military cyber commanders, to precisely identify and engage specific threats and targets with a high confidence of success. Provides a disproportionate advantage for cyber operational modeling,			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense		Date: May 2021
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
within high variability architectures. These advantages impact industrial control systems and critical infrastructures across blue, gray, and red spaces. Applied Mathematics for Cyber: Advancements in cyberspace-relevant mathematics cut across all three thrust areas producing new provable methods to design, secure, and reason about complex cyber systems. There is a need for an array of formal and informal modeling techniques, backed by various rigorous mathematical theories, to capture and support the richness of the cyber domain. ***FY 2021 Plans:*** Behavioral Cyber Science: - Demonstrate prototype of Contextualized Operator Perspective work support system, measuring increase in Cyber Protection Team (CPT) efficiency via field exercises or at DreamPort. Impact: Achieve a support system for CPT planning, network operations, and situational awareness. Increase CPT efficiency by 2x. Self-Securing Systems: - Demonstrate and quantify a cyber-resilient command and control (C2) software defined network architecture in the U.S. Army's C2/Internet of Battle-Things environment. Pilot on Department of Defense Information Networks (DoDIN). Impact: Achieve autonomic cyber-resilience that self-hardens up to 1000x faster than current human-mediated responses (~days). - Develop ground vehicle threat and mitigation scenario, to highlight existing countermeasures to supply chain threats as part of an overall cyber resilience demonstration. Calibrate metrics to help evaluate the efficacy of combined/integrated defense techniques on simulated vehicle. Impact: Implementation of a system that uses automated reasoning to evolve securely to changes in an attacker's behavior, yielding resilience beyond limitations in current vehicle signature-based detection methods. - Consolidate data from DoD Cybersecurity S&T investment areas that address gaps and accelerate the adaptation of promising results into military vehicle platforms and commercial vehicles. The integration of the results will leverage both commercial and Government investments, to ensure solutions introduce a pipeline and supply chain, supporting adaptation. Plan for four (4) Cyber-Day construct demonstrations. Impact: Accelerate the transition of DoD S&T cybersecurity technologies into military ground vehicles and commercial fleets that serve military critical missions. Precise Cyber Effects: - Demonstrate cyber-physical system dependency using Modeling and Simulation (M&S) based discovery, and integrate improved discovery process into evolving Cyber Joint Munitions Effectiveness Manual (JMEM) within the operations community. Impact: Achieve repeatable methodology to estimate scope and severity of cyber effects, reducing uncertainty risks associated with offensive planning - improved viability will enhance model functional dependencies fundamental to estimating cyber operational risks.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense		Date: May 2021
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Applied Mathematics for Cyber: - Explore the use AI as a force multiplier to enhance human-machine teaming for robust decision-making, Develop AI-Augmented capabilities across Cyber-Kill chain, Build Autonomous Cyber Defense capabilities and Development of AI-Enabled Technologies for Cyber. Impact: These efforts will provide tools to outmaneuver the adversary in cyberspace; monitor and anticipate threats in real time, build trustworthy AI defenses for Cyber and faster AI model training and testing for Cyber. ***FY 2022 Plans:*** Plan for new research efforts to identify and meet objectives under the thrust areas of Behavioral Cyber Science, Self-Securing Systems, Precise Cyber Effects, and Applied Mathematics for Cyber. These efforts will explore challenges in applied research in topics such as Artificial Intelligence/Machine Learning; Countering Adversarial Machine Learning; Exploring Precise Cyber Effects at the tactical edge; and DoD cyber work force training and education. Self-Securing Systems: - Integrate formal methods into a high security and high agility DevSecOps development process. Impact: The process will help meet Departmental goal of rapidly fielding software to serve as a trust foundation for increasingly cyber resilient systems. Precision Cyber Effects: - Expand existing cyber funded research, to add ensembles helping to reduce uncertainty surrounding predicted effect types and their measured magnitudes within critical infrastructures. Examining statistics-based methods to develop more robust causality models of system performance and failure. Impact: Improved viability and utility of OCO; More precise cyber testing and verification of blue systems Applied Mathematics for Cyber: - Explore the technical rigors, science-based, repeatable, automated, and affordable methods for quantitatively measuring cyber resilience offered to military engineered artifacts. Impact: Provides quantifiable and repeatable measures for mission resilience to guide development or assessment decisions ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Changes reflect minor budget fluctuations.			
Accomplishments/Planned Programs Subtotals	14.454	15.245	15.380

	FY 2020	FY 2021
Congressional Add: Cyber Institutes at Institutions of Higher Learning	10.000	10.000
FY 2020 Accomplishments: Conducted “listening sessions” with potential stakeholders in education and defense sectors to identify and assess existing cyber education programs, as well as current and future		

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense		Date: May 2021
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

	FY 2020	FY 2021
workforce needs. Developed Plan of Action and Milestones to establish a new "Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ" (VICEROY) program to meet the Congressional mandate of "accelerating and focusing the development of foundational expertise in critical cyber operational skills for future military and civilian leaders of the Armed Forces and the Department of Defense." Selected non-profit partnership intermediary to administer the VICEROY program and engage academia on our behalf. Obligated funds under a Partnership Intermediary Agreement and issued a special notice soliciting proposals for the first cohort of VICEROY cyber institutes. Anticipated awards stemming from this special notice made in 2Q FY 2021. ***FY 2021 Plans:*** - Complete sub-awards for FY 2020 VICEROY Institutes cohort by 2Q FY 2021. The cross service/component source selection team evaluated proposals to identify top candidates under the first tranche of funding, with execution beginning in 3Q FY 2021. - Develop and release a solicitation for FY 2021 proposals from higher learning institutes interested joining the virtual cyber institutes cohort. Post solicitation in 2Q FY 2021 with the goal of completing the sub-awards in 3Q FY 2021. - Convene first VICEROY symposium in Q4 FY 2021 to connect virtual institute member organizations with the DoD governance board. Symposium planned as an in-person event but in the event of COVID-19 restriction will move to alternative virtual event.		
Congressional Adds Subtotals	10.000	10.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A