Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Office of the Secretary Of Defense	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	14.429	14.594	25.118	15.255	-	15.255	15.586	15.857	16.265	16.596	Continuing	Continuing
003: *Cyber Applied Research*	14.429	14.594	25.118	15.255	-	15.255	15.586	15.857	16.265	16.596	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cybersecurity Applied Research program (PE: 0602668D8Z) promotes innovative higher risk cyber research to address joint force challenges in full spectrum cyber operations. Through the dedicated funding line 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 NDS, DoD Cyber Strategy, and Office of Under Secretary of Defense for Research and Engineering (OUSD(R&E)) 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. Developing research thrusts areas in: Behavior Cyber Science, Self-Securing Systems, Precise Cyber Effects, and Applied Mathematics for Cyber.

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	14.935	15.118	15.396	-	15.396
Current President's Budget	14.594	25.118	15.255	-	15.255
Total Adjustments	-0.341	10.000	-0.141	-	-0.141
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	10.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.338	-			
• Other Adjustments	-0.003	-	-0.126	-	-0.126
• Economic Assumption	-	-	-0.015	-	-0.015

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2019	FY 2020
Project: 003: *Cyber Applied Research*		
Congressional Add: *Leveraging Next Generation Cyber Joint Service Capabilities*	-	10.000
Congressional Add Subtotals for Project: 003	-	10.000
Congressional Add Totals for all Projects	-	10.000

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Office of the Secretary Of Defense	Date: February 2020
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602668D8Z *I Cyber Security Research*

Change Summary Explanation

FY 2021 increase in $10.000 million for Leveraging Next Generation Cyber Joint Service Capabilities.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
003: *Cyber Applied Research*	14.429	14.594	25.118	15.255	-	15.255	15.586	15.857	16.265	16.596	Continuing	Continuing

A. Mission Description and Budget Item Justification

As adversaries develop more sophisticated technology and tactics and become more skilled and better funded, the cyber S&T community must accelerate the pace of innovative research. Judiciously exploring research under these thrust areas should provide a distinct advantage in future cyber conflicts. Following a review and assessment of emerging joint operational needs, OUSD(R&E) developed four (4) research areas to enhance the DoD's tactical edge in a rapidly evolving cyber domain (described below):

• Behavioral Cyber Science: Exploring the interaction between computers and human behavior by moving beyond binary electronic signals towards understanding human behavior. New insights from behavioral science will increase the effectiveness of tools, increase the effectiveness of the cyber workforce, and improve the utility of cyber solutions. Behavioral cyber science seeks to uncover details about how humans (represented by operators, users, adversaries, and/or defenders) react to cyber actions and how those reactions can be understood, from a behavioral science standpoint, and leveraged to create more effective actions and outcomes.

• Self-Securing Systems: Prevailing in a contested cyber environment will require new sciences and mechanisms for autonomous cybersecurity to protect the increasingly complex weapon systems and platforms that help DoD operators react more quickly to cyber-attacks. Exploring foundational research in self-securing systems will arm future DoD systems with the capability to proactively, autonomously, and seamlessly assess cyber threats. Additionally, future systems will be able to deploy self-defense mechanisms to neutralize cyber-attacks and enable blue forces to maneuver at will. Autonomous cyber defenses will need to apply the most current advances in artificial intelligence research.

• Precise Cyber Effects: Precision offensive campaigns for the cyber domain require accurate and timely predictions of cyber effects to enable DoD leadership to achieve the desired outcomes from cyber operations and help manage risks associated with collateral damage. Exploring methods to derive quantifiable metrics will help improve the precision control of selecting cyber mission targets and raise the accuracy of effects; achieving an understanding of second and third order of effects will provide commanders with a higher confidence of success and limit collateral damage.

• Applied Mathematics for Cyber: Advancing mathematical foundations that are intrinsically linked to all branches of cyber science and technology, will cut across focus areas producing new methods to design, secure, and reason about complex cyber systems. This area of research will characterize the cyber domain, maintain the integrity of data, harden systems, analyze potential solutions, and counter adversarial machine learning.

Advances in these cyber S&T areas will promote strong foundations, while disruptive innovations will create surprise, shape the fight, and ensure a decisive advantage. The research areas are critical to the development of innovative and sustainable research that takes cybersecurity beyond the incremental escalation of attack and defense.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Leveraging Next Generation Cyber Joint Service Capabilities	14.594	15.118	15.255

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
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 2019	FY 2020	FY 2021
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. 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. By focusing on higher risk research ideas with major potential impacts, the Cybersecurity program addresses one of the NDS's mission focus areas of cybersecurity. The program works to advance the state of cybersecurity by judiciously exploring research in the areas of Behavioral Cyber Science; Self-Securing Systems; Precise Cyber Effects; and Applied Mathematics for Cyber. These thrusts provide an opportunity to identify and advance foundational technologies to support all Services and Agencies. Research in Behavioral Cyber Science advances understanding and the technical rigor of modeling and predicting human responses to cyber activities that enhance cyber operations through planning, and training. Exploring the interaction between computers and human behavior, moving beyond electronic signals (ones and zeroes) enables development of new insights to human behavior. Exploring Self-Securing Systems, platforms, and networks will help DoD operators react more quickly to cyber-attacks. Equipping 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 provide scalable cyber options for military cyber commanders to precisely identify and engage specific threats and targets with a high confidence of success. This high-risk research provides a disproportionate advantage in modeling cyber with high variability architectures for blue, gray, and red space that would potentially afford real opportunities. Finally advancements in mathematical foundations of cyber 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 2020 Plans:*** Performance Assessment Suite for Cyber Mission Force project will integrate research automated for predictive analytics into Joint Artificial Intelligence Center (JAIC) rapid prototyping events at Dreamport. Research will develop a prototype for workflow monitoring, addressing human-in-the-loop protocols by refining simulation-based software. (Behavioral Cyber Science) Robust Low-level Cyber Attack-Resilience for Warfighting Vehicles project will develop new attack scenarios/patterns developed through Artificial Intelligence/Machine Learning (AI/ML) based intrusion detection simulators to harden vehicle security. (Self-Securing Systems) Autonomous Cyber Defense project will demonstrate a prototype of autonomous cyber defense using deception techniques based on human operator defender goals. The demonstration will test and simulate different AI techniques, using both deception and cyber defense tactics. (Self-Securing Systems)			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
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 2019	FY 2020	FY 2021
Fifth Generation (5G) Secure Co-existence of Advanced Networks (SCAN) project will examine 5G security issues and spectrum opportunities to augment Future Autonomous Battlespace Radio Frequency (RF) with Integrated Communications (FABRIC). (Precise Cyber Effects) Stealthy Communications and Situational Awareness project will develop Linear Statistical Network Analysis (LSNA) infused Naval Research Laboratory Extensible Stealthy Protocol (NExtSteP) test-bed and determine the “stealthiness” of throughput, to ensure consistency with the proof-of-concept overlay protocol.(Applied Mathematics) Mitigating Adversarial Machine Learning project will investigate evasion, inversion, and extraction attack techniques to enhance the performers understanding of machine learning resilience and its effects on human operator decision support. (Applied Mathematics) ***FY 2021 Plans:*** Plan for new research efforts to identify and meet objectives under the thrust areas. A list of some of the research under consideration is: Artificial Intelligence/Machine Learning (AI/ML); Countering Adversarial Machine Learning; 5G Vulnerabilities; Exploring 6G Standards; and Exploring Precise Cyber Effects at the Tactical Edge. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Level of effort is consistent between FY 2020 and FY 2021. Small changes reflect minor budget fluctuations.			
Accomplishments/Planned Programs Subtotals	14.594	15.118	15.255

	FY 2019	FY 2020
Congressional Add: Leveraging Next Generation Cyber Joint Service Capabilities	-	10.000
FY 2020 Plans: Initiate and harness research opportunities in academic cyber institutes. The effort will leverage existing partnerships with academia to reduce vulnerabilities in our national information infrastructure by promoting higher education, workforce development, and research in cyber defense. These investments will establish mechanisms / foundries for future learning and increase the professional workforce with cyber defense expertise. These efforts will promote investments in key cyber areas at these institutions.		
Congressional Adds Subtotals	-	10.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

D. Acquisition Strategy

N/A