Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense	Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
Total Program Element	-	24.328	25.331	17.264	0.000	17.264	17.744	18.115	18.510	18.881	Continuing	Continuing
003: *Cyber Applied Research*	-	24.328	25.331	17.264	0.000	17.264	17.744	18.115	18.510	18.881	Continuing	Continuing

Note

New Start (Y/N): No

A. Mission Description and Budget Item Justification

This program supports the Department's initiatives to Defend the Homeland and Build Sustainable and Long-Term Advantage.

The Cyber Security Applied Research program element promotes innovative higher risk cyber research to meet 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)) strategic cyber capability goals, the program recalibrated research thrust areas to emphasize the role of electromagnetic spectrum operations (EMSO) and artificial intelligence as key enablers for cyber power projection of scale, speed, and dominance. The established research thrusts areas are: Behavioral Cyber Applied Research, Self-Securing Systems, Precise Cyber-EMSO Effects, and Applied Mathematics for Cyber.

B. Program Change Summary ($ in Millions)	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total
Previous President's Budget	25.245	15.380	0.000	0.000	0.000
Current President's Budget	24.328	25.331	17.264	0.000	17.264
Total Adjustments	-0.917	9.951	17.264	0.000	17.264
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	10.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.912	-			
• Other Reprogramming	-0.005	-	-	-	-
• FFRDC	-	-0.049	-	-	-
• Adjustments to Budget Year	-	-	16.668	-	16.668
• Economic Assumption	-	-	0.596	-	0.596

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense	Date: April 2022
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*

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2021	FY 2022
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

Change Summary Explanation

FY 2022 funding increase reflects $10.000 million Congressional add for Academic Cyber Institutes.

FY 2023 funding increase reflects the fact that the FY 2022 President’s Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
003: *Cyber Applied Research*	-	24.328	25.331	17.264	0.000	17.264	17.744	18.115	18.510	18.881	Continuing	Continuing

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, the development of the USD(R&E) S&T Strategy for Cyber, and the 2021 Interim National Security Strategic Guidance.

This 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 Applied Research; Self-Securing Systems; Precise Cyber-EMSO 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 2021	FY 2022	FY 2023
Title: OUSD(R&E) Cyber Technologies	14.328	15.331	17.264
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. Behavioral Cyber Applied Research: 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, resistance to adversarial cyber influence, and cyber situational awareness. 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-EMSO Effects: Provides scalable cyber options for military cyber commanders, to precisely identify and engage specific threats and targets with a high confidence of success. Identifies early cyber-EMSO integration opportunities and			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
advances technology to support future prototypes and assessments. Provides a disproportionate advantage for cyber operational modeling, 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 such as machine learning and artificial intelligence 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. These collective capabilities are fundamentally crucial for DoD to achieve dominance in cyber situation awareness, decision-making, and automated implementation of courses of action. ***FY 2022 Plans:*** - Complete projects initiated in FY 2021, as well as initiate new projects that consider the implication of the NDAA FY 2021 Section 257 DoD 25-Year Roadmap for Cyber. These efforts will explore challenges in applied research topics, such as Artificial Intelligence/Machine Learning; Countering Adversarial Machine Learning; Exploring Precise Cyber-EMSO Effects at the tactical edge; and DoD cyber work force operational planning and execution, training, and education. Self-Securing Systems: - Design and develop intrusion prevention systems with technologies that support ground vehicle cybersecurity, while employing critical technology focusing on peer to near-peer threats. Integrate DoD cybersecurity S&T investment areas in order to address shortfalls, gaps and accelerate/advance results for adaptation and insertion into military and commercial platforms and supply chains. Impact: The process will help meet the Department's goal of rapidly fielding software and hardware to serve as a trust foundation, resulting in increasingly cyber resilient systems, while building solutions for sustainment of supply chain security. Precise Cyber-EMSO Effects: - Enhance ongoing Critical Infrastructure Protection cyber research to reduce uncertainty surrounding predicted effect types and their measured magnitudes within electrical energy distribution networks. - Refine 5G vulnerability analysis framework to more precisely assess blue 5G systems and rapidly identify vulnerabilities within 5G core and radio access network software. Develop prototype 5G effects framework suitable for experimentation and assessment. Impact: Clear understanding of impact and risk of using 5G core services for specific DoD capabilities. Prototype 5G effects framework whose technology will be transitioned to the 16th Air Force for future enhancement. Behavioral Cyber Applied Research: - Complete Contextualized Operator Perspective project. Demonstrate to USCYBERCOM and other stakeholders, with intent to technically transition into Joint Cyber Command and Control program.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
- Release a call for targeted proposals for creating new insights to increase effectiveness of tools, cyber workforce, and cyber solutions for large scale DoD operations. Impact: Increase tempo, scale, and complexity of cyber operations via increased operator efficiency. Applied Mathematics for Cyber: - Complete projects initiated in FY 2021, as well as initiate new projects that consider the implication of the Cyber Roadmap Working Group's report on the NDAA FY 2020 Section 257 DoD 25-Year Roadmap for Cyber. These efforts will explore challenges in applied research topics, such as Artificial Intelligence/Machine Learning; Countering Adversarial Machine Learning; Exploring Precise Cyber-EMSO Effects at the tactical edge; and DoD cyber work force operational planning and execution, training, and education. Self-Securing Systems: - Design and develop intrusion prevention systems with technologies that support ground vehicle cybersecurity, while employing critical technology focusing on peer to near-peer threats. Integrate DoD cybersecurity S&T investment areas in order to address shortfalls, gaps and accelerate/advance results for adaptation and insertion into military and commercial platforms and supply chains. Impact: The process will help meet the Department's goal of rapidly fielding software and hardware to serve as a trust foundation, resulting in increasingly cyber resilient systems, while building solutions for sustainment of supply chain security. Precise Cyber-EMSO Effects: - Enhance on going Critical Infrastructure Protection cyber research to reduce uncertainty surrounding predicted effect types and their measured magnitudes within electrical energy distribution networks. - Refine 5G vulnerability analysis framework to more precisely assess blue 5G systems and rapidly identify vulnerabilities within 5G core and radio access network software. Develop prototype 5G effects framework suitable for experimentation and assessment. Impact: Clear understanding of impact and risk of using 5G core services for specific DoD capabilities. Prototype 5G effects framework whose technology will be transitioned to the 16th Air Force for future enhancement. Behavioral Cyber Applied Research: - Complete Contextualized Operator Perspective project. Demonstrate to USCYBERCOM and other stakeholders, with intent to technically transition into Joint Cyber Command and Control program. - Release a call for targeted proposals for creating new insights to increase effectiveness of tools, cyber workforce, and cyber solutions for large scale DoD operations. Impact: Increase tempo, scale, and complexity of cyber operations via increased operator efficiency. Applied Mathematics for Cyber:			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
- Develop a novel technique for integrating formal methods into a modern DevSecOps development process, reduce certification risk by piloting methods on DoD Platform One, and validate with the Navy's Strategic Systems Program. Impact: Increase the speed and rigor of cybersecurity analysis within Air Force and Navy DevSecOps processes. - Develop lab-based prototype system to measure the cyber-resilience of military vehicle systems, with Army's Combat Capabilities Development Command (CCDC), Army Research Laboratory (ARL). - Develop a proof-of-concept system for AI-powered automated mitigations to counter-autonomy threats associated with robotic and autonomous system cybersecurity attacks wit contribution from Cybersecurity for Robotic & Autonomous Systems Hardening and Joint Capability Technology Demonstrations. Impact: Reduces cyber risk to Cybersecurity for Robotic & Autonomous Systems Hardening (CRASH) Joint Capability Technology Demonstrations (JCTD) by providing quantifiable and repeatable measures for mission resilience to guide development or assessment decisions also rapidly fielding software and hardware.			
FY 2023 Plans: - Revector Cyber PE investments consistent with the updated 2022 National Defense Strategy and anticipated DoD Cyber Strategy. Consider revision of four main thrust areas, Behavioral Cyber Applied Research, Self-Securing Systems, Precise Cyber-EMSO Effects, and Applied Mathematics for Cyber, if needed. - Emphasize the early and deep integration and acceleration of Cyber and Electromagnetic Spectrum Operations (EMSO) S&T capabilities within the Services and Components. Complete Cyber-EMSO integration opportunity roadmap. Complete Cyber-EMSO S&T Landscape Analysis and Roadmap. - Fund and accelerate select Cyber-EMSO integrated concepts that project power through the Information, Cyber, and Spectrum domains in tight coordination, leveraging Internet of Things opportunities. - Transition automated Fifth Generation (5G) core vulnerability analysis capabilities to 16th Air Force and other DoD organizations. - Continue completion of FY 2022 projects in the areas of Applied Mathematics for Cyber and Behavioral Cyber Applied Research thrust areas. - Deliver engagement strategy and roadmap for DoD to engage ground vehicle Original Equipment Manufacturers for transition of DoD automated resilience technologies. - Launch new S&T exploring security concerns within cellular Sixth Generation (6G) standards. - Transition automated Fifth Generation (5G) core vulnerability analysis capabilities to 16th Air Force and other DoD organizations. - Continue completion of FY 2022 projects in the areas of Applied Mathematics for Cyber and Behavioral Cyber Applied Research thrust areas. - Deliver engagement strategy and roadmap for DoD to engage ground vehicle Original Equipment Manufacturers for transition of DoD automated resilience technologies. - Launch new S&T exploring security concerns within cellular Sixth Generation (6G) standards.			
FY 2022 to FY 2023 Increase/Decrease Statement:			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
The additional resources will be used to strategically target new investments areas aligned with the National Defense Strategy and DoD Cyber Strategy for FY 2022.			
Accomplishments/Planned Programs Subtotals	14.328	15.331	17.264

	FY 2021	FY 2022
Congressional Add: Cyber Institutes at Institutions of Higher Learning	10.000	10.000
FY 2021 Accomplishments: - Completed 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. - Developed and released a solicitation for FY 2021 proposals from higher learning institutes interested in joining the virtual cyber institutes cohort. Posted solicitation in 2Q FY 2021 with the goal of completing the sub-awards in 3Q FY 2021. - Convened first VICEROY symposium in 4Q FY 2021 to connect virtual institute member organizations with the DoD governance board		
FY 2022 Plans: - Complete source selection for next cohort of awards in December 2021, with sub-awards for three new VICEROY institutes anticipated to be finalized in early April 2022. - The Air Force Research Laboratory's Information Directorate will host VICEROY's first, eight Week "Introduction to Cyber" summer internship program. - The VICEROY program management team will continue to work with Congress and awarded schools to identify opportunities to expand the program, accelerate expenditure of funding, and provide longer-term student support.		
Congressional Adds Subtotals	10.000	10.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A