Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Office of the Secretary Of Defense	Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
Total Program Element	48.915	41.258	17.437	17.652	-	17.652	18.046	18.421	18.824	19.200	Continuing	Continuing
003: *Cyber Applied Research*	48.915	41.258	17.437	17.652	-	17.652	18.046	18.421	18.824	19.200	Continuing	Continuing

Note

New Start (Y/N): No

A. Mission Description and Budget Item Justification

This Program Element supports the Department's National Defense Strategy priorities to Defend the Homeland, Deter Strategic Attacks against the United States, Deterring Aggression, and Building a resilient Joint Force and defense ecosystem.

The Cyber Security Applied Research program 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 by integrating 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 effort recognizes the role of electromagnetic spectrum operations (EMSO) and artificial intelligence as key enablers for cyber power projection mass, maneuver, and unity of command for dominance. The research thrusts areas are: Augmented Cognition, Dominant Cyber Operations, Dependable Systems and Networks, and Cyber Foundations.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	42.139	17.437	17.794	-	17.794
Current President's Budget	41.258	17.437	17.652	-	17.652
Total Adjustments	-0.881	0.000	-0.142	-	-0.142
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.881	-			
• Program Adjustment	-	-	-0.142	-	-0.142

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2023	FY 2024
Project: 003: *Cyber Applied Research*		

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Office of the Secretary Of Defense	Date: March 2024
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 2023	FY 2024
Congressional Add: *Cyber Institutes at Institutions of Higher Learning (VICEROY)*	10.000	-
Congressional Add: *University Consortium for Cybersecurity (UC2)*	10.000	-
Congressional Add: *Pacific Intelligence and Innovation Initiatives (PI3)*	5.000	-
Congressional Add Subtotals for Project: 003	25.000	-
Congressional Add Totals for all Projects	25.000	-

Change Summary Explanation

FY 2023 prior year changes due to SBIR/STTR calculations

Program Adjustments for FY 2025 a reduction of $0.178 was applied to meet DoD overall funding reductions, which were spread to mitigate impact.

Funding increase of $0.036 million for Economic Assumptions.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense			Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
003: *Cyber Applied Research*	48.915	41.258	17.437	17.652	-	17.652	18.046	18.421	18.824	19.200	Continuing	Continuing

A. Mission Description and Budget Item Justification

Cyberspace, as an operational domain, creates both significant security and resilience challenges for the joint force, as well as potential leap-ahead capabilities for military operations. Cyber is often used both to designate that domain and as shorthand for the set of technologies that enable operations in and through cyberspace, such as command-and-control, situational awareness, software analysis and hardening, and autonomy/Artificial Intelligence (AI) applications. The U.S. must maintain technological advantage in cyberspace despite a rapidly evolving globally driven commercial landscape and supply chain, and a set of determined and highly capable adversaries, to maintain mission readiness and deter conflict. The 2022 National Defense Strategy recognizes the “growing kinetic and non-kinetic threat to the United States’ homeland from our strategic competitors, “requiring the Department to “withstand, fight through, and recover quickly from disruption” embracing technology, resiliency, and innovation to act at scale and speed” as key components for all cyber efforts. The DoD will accelerate the development of those cyber capabilities that benefit our warfighters and those cyber capabilities intended to counter malicious cyber actors. It will also seize opportunities to fully integrate spectrum and sensing technologies into future cyber capabilities, to maximize situation awareness, and enable persistent operations and agile power projection options. The DoD will focus on fielding capabilities that are scalable, adaptable, and diverse to provide maximum flexibility to joint force commanders, so the joint force retains the freedom and capability to employ cyberspace operations throughout the spectrum of conflict to advance U.S. interests.

This program focuses on higher risk research ideas with major potential impact for addressing National Defense Strategy 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 Augmented Cognition, Dominant Cyber Operations, Dependable Systems and Networks, and Cyber Foundations. Advances in these cyber science and technology thrusts will promote strong foundations, while disruptive innovations will create surprise, shape the fight, and ensure a decisive advantage. The thrusts provide an opportunity to identify and advance foundational technologies to support all services and agencies.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: OUSD(R&E) Cyber Technologies	16.258	17.437	17.652
Description: Description: Integrating both defensive and offensive innovative cyber research within the DoD cyber science and technology enterprise to develop interoperable, defense-wide technology options that address joint force challenges in full spectrum integrated sensing and cyber operations. Augmented Cognition: Integrates human ingenuity with machine intelligence, computation, and sensing technologies to extend cognitive capabilities, empower humans, and, ultimately, improve system performance. As the complexity of the cyber battlefield increases, augmented cognition can reduce cognitive workload of cyber personnel, support more effective human-machine teaming, individualize training and learning, and improve operator situation awareness, sensemaking, decision support, and communication.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
Dominant Cyber Operations: Cyber operations that embody the JP 3-0 principles of mas, maneuver, and unity of command so that they have a high probability of achieving specific outcomes with minimal collateral damage and unforeseen consequences. Operations must predict and quantify the significance of both immediate and latent higher-order effects, thus controlling the state of an intended cyber target without perturbing unintended kinetic and non-kinetic entities. Dependable Systems and Networks: Dependable systems and networks are characterized by the principles, methods, and technologies whose aim is to increase the availability, reliability, survivability, and integrity of cyber systems and networks providing critical military capabilities at the physical and logical network layers. Cyber Foundations: Provides cross-cutting opportunities across the other thrusts by promoting applied mathematics research on formal cyber proofing methods and securing data in transit. The evaluation and measurement tools that characterize CF underpin development and enable key breakthroughs in multiple fields of cyber research. ***FY 2024 Plans:*** - Emphasize the early and deep integration and acceleration of Cyber, Sensing, and Electromagnetic Spectrum Operations (EMSO) science and technology capabilities within the services and components. - Explore concepts of information advantage across the non-kinetic effects domains of cyber, EMSO, and cognitive/information. - Support development of a non-kinetic force employment strategy through integrated Cyber-EMSO capabilities, and support Operations in the Information Environment. - Kringle Mingle's Artificial Intelligence/Machine Learning (AI/ML) Internet of Things Monitoring System was successfully tested, and the code base updated to allow the platform to be used for a variety of situations other than just a distributed building monitoring system. Significant work is on-going to add Kringle Mingle's AI/ML anomaly detection algorithms to transition partner National Security Agency R4's spectrum monitoring platform. - The Development Security Operations (DevSecOps) effort has successfully integrated to Sonatype Lift, a DevSecOps platform for integrating analysis tools with development workflow, into one of Navy SSP's isolated networks. This is the first step for getting Navy teams using Lift on their own projects and transition efforts continue to integrate Lift with the Dahlgren software assurance and software factory teams. - Deliver engagement strategy and roadmap for DoD to engage ground vehicle Original Equipment Manufacturers for transition of DoD automated resilience technologies. - Work with interagency partners to draft an Interagency Task Force / Program Management Office terms of reference, that will formalize cooperation and coordination of ground vehicle security initiatives. Provide proposed input to FY 2024 NDAA - Deliver technical and analytical cyber support in researching, authoring, producing reports and analyses of existing and future full spectrum cyber operations. Assessing R&D programs and their impact on DoD information systems architectures.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Transition automated Fifth Generation (5G) core engagement architecture and capabilities to 16th Air Force and other DoD organizations ***FY 2025 Plans:*** - Augmented Cognition: Develop capabilities that enhance USCYBERCOM and Service Cyber Components' ability to increase the scale and scale of human operators in comprehending, planning executing, and assessing operations. - Dependable Systems and Networks: Develop secure hardware and software co-design that will enable development of provably secure systems at scale, design, and architecture. Cyber-physical digital-twins systems can be used to develop secure hardware/ software co-design standards with full stack visibility enabled by supply chain analysis. - Dominant Cyber Operations: Develop cyber warfighting concepts and demonstrable capabilities that integrate with electromagnetic warfare, intelligence, and kinetic operational planning and execution. Demonstrate concepts integrated within a cyber-flag or red-flag level exercise to illustrate potential/impact. - Cyber Foundations: Explore formal methods for rigorous mathematical specification and verification of cyber hardware and software systems. Industrial scale formal methods and related techniques have the potential for greatly reducing the uncertainty in the software used in military systems. - Manipulate spatial beam qualities to demonstrate laser system propagation in outdoor atmospheric environments to achieve desired effects on sensors. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The increase of $0.215 million between FY 2024 and FY 2025 will target seedlings in new investments areas aligned with the National Defense Strategy and DoD Cyber Strategy.			
Accomplishments/Planned Programs Subtotals	16.258	17.437	17.652

	FY 2023	FY 2024
Congressional Add: Cyber Institutes at Institutions of Higher Learning (VICEROY)	10.000	-
FY 2023 Accomplishments: -VICEROY grew to a total of 498 graduate and undergraduate students. (Reserve Officers' Training Corps – 112; Female – 142; Minority – 122). The program doubled the number of virtual institutes from 6 to 13, encompassing 45 post-secondary institutions. -VICEROY developed a summer internship program called MAVEN, where it doubled internships from 22 to 48 student participants. MAVEN mission-focused capstone models Air Force Unit Cyber Warfighting Training scenario.		

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

	FY 2023	FY 2024
-VICEROY developed 13 new undergraduate courses and one new masters program, with over 50 student research projects completed across the entire consortium. -The program signed memorandums of agreement with 4 DoD internship host sites with more expected later this year. There are currently 34 DoD participating organizations and growing monthly.		
Congressional Add: University Consortium for Cybersecurity (UC2) ***FY 2023 Accomplishments:*** -The Consortium issued three requests for information to the broader UC2 community. Funding for UC2 will incentivize and fund more than 360 institutions of higher learning to respond to Requests for Information from the Secretary of Defense, through the National Defense University. -The consortium funded three solution concepts.	10.000	-
Congressional Add: Pacific Intelligence and Innovation Initiatives (PI3) ***FY 2023 Accomplishments:*** - Pacific Intelligence and Innovation Initiatives (P3I) Executed numerous sub-agreements with HII partners in secondary schools, chamber of commerce, and military organizations - P3I is establishing summer internship opportunities - P3I will refine and promote curriculum programs with increased certificate offerings	5.000	-
Congressional Adds Subtotals	25.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A