Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Office of the Secretary Of Defense	Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
Total Program Element	24.328	24.587	42.139	17.437	-	17.437	17.794	18.194	18.574	18.980	Continuing	Continuing
003: *Cyber Applied Research*	24.328	24.587	42.139	17.437	-	17.437	17.794	18.194	18.574	18.980	Continuing	Continuing

Note

New Start (Y/N): No

A. Mission Description and Budget Item Justification

This program 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 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: Augmented Cognition for Cyber Operations, Precision Cyber Operations, Applied Mathematics for Cyber, and Dependable Systems and Networks.

B. Program Change Summary ($ in Millions)	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total
Previous President's Budget	25.331	17.264	17.744	-	17.744
Current President's Budget	24.587	42.139	17.437	-	17.437
Total Adjustments	-0.744	24.875	-0.307	-	-0.307
• Congressional General Reductions	-	-0.125			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	25.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program Adjustments	-0.744	-	-0.307	-	-0.307

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Office of the Secretary Of Defense	Date: March 2023
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 2022	FY 2023
Project: 003: *Cyber Applied Research*		
Congressional Add: *Cyber Institutes at Institutions of Higher Learning (VICEROY)*	10.000	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	10.000	25.000
Congressional Add Totals for all Projects	10.000	25.000

Change Summary Explanation

The FY 2022 decrease of $0.744 million was attributed to a realignment of funds to support high priority Under Secretary of Defense for Research and Engineering (USD(R&E)) initiatives.

The FY 2023 increase was an addition of $25.000 million to fund three research efforts under the Cyber Research Program. $10.000 million was added as a continuation of the R&E VICEROY program that provides sustainment funds for existing Institutes, an additional $10M allotment was added for research seedlings to incentivize university participation and transfer of innovations through the University Consortium for Cybersecurity (UC2), and the final addition was for a $5M program increase to support a Pacific Intelligence and Innovation Initiative.

The FY 2024 decrease of $0.307 million is attributed to the realignment of $0.368 million to support the Historically Black Colleges and Universities/Minority Serving Institutions program, $0.019 million to support departmental priorities and an economic assumption increase of $0.098 million.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense											Date: March 2023	
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**Cost To Complete**	**Total Cost**
003: *Cyber Applied Research*	24.328	24.587	42.139	17.437	-	17.437	17.794	18.194	18.574	18.980	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, 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/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, in order to maintain mission readiness and deter conflict. The 2018 DoD Cyber2022 National Defense Strategy highlights 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 also 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, 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 in order to advance U.S. interests

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 Augmented Cognition for Cyber Operations, Precision Cyber Operations, Applied Mathematics for Cyber, and Dependable Systems and Networks. 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 2022**	**FY 2023**	**FY 2024**
Title: OUSD(R&E) Cyber Technologies	14.587	17.139	17.437
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. Augmented Cognition for Cyber Operations: Improve a cyber operator's ability to make evidence-based decisions and act in a cyber domain characterized by ever increasing size, speed, and complexity. Augmented cognition is focused on adapting, improving, and increasing the cognitive capacity and capabilities of cyber operators through artificial enhancements. These			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
enhancements may be external, such as through computational means (e.g., intelligent agents), or internal, such as through behavioral (e.g., training and education) or physical (e.g., intercranial stimulation) means. Precision Cyber Operations: Improvement of cyber offensive and defensive capabilities by increasing the likelihood of the cyber operator achieving the desired effect while minimizing collateral damage. Integrates sensing and electromagnetic spectrum technologies to increase operational agility, speed, and accuracy. Effects from a proposed courses of action should be quantified and supported by subjective evidence. 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, assess, 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, automating implementation of courses of action, and delivering cyber capabilities at the speed of need. Dependable Systems and Networks: Increase the availability, reliability, survivability and integrity of cyber systems and networks providing critical military capabilities from design faults, natural component failures, and effects stemming from adversarial cyber attacks. ***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. - Initiate Interagency Task Force for Ground Vehicle Cybersecurity for DoD and Federal Gov't 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- 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 2024 Plans:*** The FY 2023 Cyber PE investment strategy was revectored consistent with the updated 2022 National Defense Strategy and anticipated DoD Cyber Strategy. As a result, the four main thrust areas highlighted in Sections A and B were revised to Augmented Cognition for Cyber Operations, Precision Cyber Operations, Applied Mathematics for Cyber, and Dependable Systems and Networks. FY24 plans will be completed based on the revised description of each thrust: - Augmented Cognition for Cyber Operations: Improve a cyber operator's ability to make evidence-based decisions and act in a cyber domain characterized by ever increasing size, speed, and complexity. Augmented cognition is focused on adapting, improving, and increasing the cognitive capacity and capabilities of cyber operators through artificial enhancements. These enhancements may be external, such as through computational means (e.g., intelligent agents), or internal, such as through behavioral (e.g., training and education) or physical (e.g., intercranial stimulation) means. - Precision Cyber Operations: Improvement of cyber offensive and defensive capabilities by increasing the likelihood of the cyber operator achieving the desired effect while minimizing collateral damage. Integrates sensing and electromagnetic spectrum technologies to increase operational agility, speed, and accuracy. Effects from a proposed courses of action should be quantified and supported by subjective evidence. - 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, assess, 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, automating implementation of courses of action, and delivering cyber capabilities at the speed of need. - Dependable Systems and Networks: Increase the availability, reliability, survivability and integrity of cyber systems and networks providing critical military capabilities from design faults, natural component failures, and effects stemming from adversarial cyber-attacks. FY 2024 Plans: - Emphasize the early and deep integration and acceleration of Cyber, Sensing, and Electromagnetic Spectrum Operations (EMSO) S&T capabilities within the Services and Components.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- Explore concepts of information advantage across the non-kinetic effects domains of cyber, EMSO, and cognitive/information. The primary focus will be on IoT targets within several of the RDER focused scenarios. - Deliver Cyber-EMSO S&T engagement strategy to support Operations in the Information Environment. - Continue completion of FY 2023 projects in the areas of Augmented Cognition for Cyber Operations, Precision Cyber Operations, Applied Mathematics for Cyber and Dependable Systems and Networks. - 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 FY2024 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. - Transition automated Fifth Generation (5G) core vulnerability analysis capabilities to 16th Air Force and other DoD organizations ***FY 2023 to FY 2024 Increase/Decrease Statement:*** The increase of $0.298 million between FY 2023 and FY 2024 will be used to strategically target new investments areas aligned with the National Defense Strategy and DoD Cyber Strategy.			
Accomplishments/Planned Programs Subtotals	14.587	17.139	17.437

	FY 2022	FY 2023
Congressional Add: Cyber Institutes at Institutions of Higher Learning (VICEROY)	10.000	10.000
FY 2022 Accomplishments: - VICEROY Virtual Institutes represent 7 of 9 National Centers of Academic Excellence in Cybersecurity Regions - VICEROY has been tailored to help bridge the workforce gap of qualified cybersecurity professionals, enrolling over 398 college students into universities to educate and prepare candidates for a career in cybersecurity supporting DoD. - VICEROY has expanded consortium to 6 regional centers composed of 22 academic institutions - The universities that are members of the VICEROY consortia, support 61 students from HBCU/MSI institutes and 139 women. - Conducted its first summer experiential internship at Air Force Research Lab ***FY 2023 Plans:*** VICEROY is projected to grow from the Air and Space Force and expand into Army and Navy.		
Congressional Add: University Consortium for Cybersecurity (UC2)	-	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

	FY 2022	FY 2023
FY 2023 Plans: 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.		
Congressional Add: Pacific Intelligence and Innovation Initiatives (PI3) ***FY 2023 Plans:*** - Pacific Intelligence and Innovation Initiatives (PI3) will establish summer internship opportunities - PI3 will refine and promote curriculum programs with increased certificate offerings	-	5.000
Congressional Adds Subtotals	10.000	25.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A