Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Office of the Secretary Of Defense	Date: February 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	14.429	14.935	15.118	-	15.118	15.396	15.662	15.956	16.294	Continuing	Continuing
003: *Cyber Applied Research*	-	14.429	14.935	15.118	-	15.118	15.396	15.662	15.956	16.294	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Applied Research program focuses on innovative and sustained research in both cybersecurity and computer network operations by developing new concepts to harden key network and computer components, designing new and resilient cyber infrastructures, increasing the military's ability to disrupt, fight and survive nation-state actors' cyber-attacks, measuring the state of health in cybersecurity, exploring and exploiting new ideas in cyber warfare for agile cyber operations and mission assurance, along with the ability to protect tactical networks, weapons systems and platforms.

This program is unique in that it integrates both the defensive and offensive cyber research from each of the Services to develop interoperable, defense-wide technology options to meet Combatant Command (CCMD) needs and requirements. More specifically, by increasing cross-laboratory collaboration, this program is able to take Service-specific technologies and expand their applications to the Joint Force.

B. Program Change Summary ($ in Millions)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	14.775	14.969	15.162	-	15.162
Current President's Budget	14.429	14.935	15.118	-	15.118
Total Adjustments	-0.346	-0.034	-0.044	-	-0.044
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.318	-			
• FFRDC Reduction	-0.028	-0.034	-	-	-
• Other Program Adjustments	-	-	-0.044	-	-0.044

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense			Date: February 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
003: *Cyber Applied Research*	-	14.429	14.935	15.118	-	15.118	15.396	15.662	15.956	16.294	Continuing	Continuing

A. Mission Description and Budget Item Justification

As adversaries develop more sophisticated technology tactics, the cyber Science and Technology (S&T) community must remain agile, vigilant, and evermore creative in response. Starting in late FY 2016, the Office of Under Secretary of Defense for Research and Engineering (USD(R&E)) reviewed new cyber threats and the emerging needs of the joint operational community. As a result, a new strategic vision was developed to enhance the DoD's tactical edge in a rapidly evolving cyber domain. Beginning in FY 2018, the following new projects were initiated in the research areas (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: 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, and analyze potential solutions.

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 2018	FY 2019	FY 2020
Title: Behavioral Cyber Science	3.614	3.750	3.753

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
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 2018	FY 2019	FY 2020
Description: The point where hardware, software, and humans interact has formed a new area of research – Behavioral Cyber Science. Research in behavioral cyber science will advance the understanding and technical rigor of modeling and predicting human responses to cyber activities which will ultimately enhance cyber operations through planning, and training. Future research must broaden the scope beyond the impacts of cyber actions on equipment to include the impact that these cyber actions will have on human behavior and our adversary's forces. Just as an adversary's behavior may be better understood using behavioral cyber science, behavioral science can be used to improve the actions of cyber defenders and the performance of the cyber workforce. Data gleaned from observing effects of various cyber operations on users' productivity, performance, and security will help the DoD design better techniques and processes for use in cyber defense and operation. ***FY 2019 Plans:*** "Performance Assessment Suite for the Cyber Mission Force" project will develop an analytics platform to accommodate future sensors, interactive data-mining, and workflow monitoring plug-ins. The initial framework for platforms will be developed for U.S. Cyber Command and tested in-house using observer tablets. Research will build a better understanding of the cyber information environment by developing Cyber Mission Force (CMF) knowledge acquisition and observational assessments. "Designing a Contextualized Operator Perspective (COP) to Enable Joint Cyber Operations" project identifies key cyber terrain, defined as the overlap between protected mission's system needs and the supporting network, to uncover potential threats for Cyber Protection Team (CPT). The discovery supports CPT analyses for developing technical and data requirements for preliminary work support systems. The research measures and explores aspects of situational awareness (SA) theory to determine the applicable methodologies to evaluate work support system designs. ***FY 2020 Plans:*** The Performance Assessment Suite project will develop a prototype of workflow monitoring, addressing human-in-the-loop protocols, by refining its design through simulation-based software. The research will document results from laboratory and capstone experiments at U.S. Cyber Command's Cyber Immersion Laboratory. Designing COP will analyze explainable artificial intelligence (XAI) to enhance the capabilities of the work support system. XAI will create a suite of machine learning techniques, enabling human users to understand, trust, and manage the emerging generation of artificially intelligent applications. Developing XAI will provide researchers with extensive search, gathering, reviewing, and assimilating capabilities. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Additional resources will be used to complete development phase of projects under the Behavioral Cyber Science thrust.			
Title: Self-Securing Systems	5.615	5.822	5.925

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
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 2018	FY 2019	FY 2020
Description: The pervasive nature of software-reliant systems in today's modern military creates new opportunities for sophisticated adversaries. The vast majority of DoD weapons systems, platforms, and networks rely on software to operate. Software can often be disrupted remotely, which necessitates a new kind of security to protect against such cyber-attacks. Defending the software and network-based aspects of critical weapon systems is challenging for a number of reasons, chief among which is the advanced nature of the adversary in the cyber realm. Future cyber adversaries will be well-funded, well-informed, and agile. Building weapon systems, platforms, and networks that defend themselves in real time will be vital in protecting ourselves against this adversary. The Department needs systems that can autonomously monitor and manage their own health and security posture through advanced sensing and perception, reasoning, and planning. Such systems identify and classify threats much more quickly than a human operator, and therefore, neutralize the threat more quickly and effectively. However, researchers must be cognizant of the potential unintended consequences of turning security over to autonomous systems. Verification techniques must be developed to ensure that autonomous and dynamic system changes maintain correct mission-focused capabilities without introducing unintended vulnerabilities. Conversely, developing techniques to track and audit actions taken by autonomous systems ensures that direct control can be reasserted. ***FY 2019 Plans:*** "Robust Low-Level Cyber Attack-resilience for Military Defense (ROLL CAGE)" will develop fast and lightweight autonomous advanced intrusion detection systems (IDS) to immediately sense anomalous behavior. Research will develop and incorporate aspects of moving target defense (MTD) and deception techniques into the IDS, based on the identification of threats. The IDS will have the ability to respond proactively to adversary actions and to detect and mitigate cyber threats. Research will explore the threat taxonomy and fine-tune development of monitoring agents under various platforms. ROLL CAGE will demonstrate system specific vulnerabilities and protection against cyber-attacks using modularized agents. These agents will establish systems operation baselines, conduct real-time monitoring, identify abnormalities, and alert users/operators of potential cyber threats and vulnerabilities. "Autonomous Intelligent Resilient Systems (AIRS)" will develop a reference architecture for command and control (C2) / Internet of Battlefield Things (IoBT) software-defined networks. The architecture allows researchers to harness the predicative analytics of intelligent command and control and battlefield services. The framework will include network topology of data and the control plane model. "Self-Securing Systems: Autonomous Cyber Defense" project will develop an autonomous cyber deception system prototype. The research will design hybrid games and hyper-games for cyber deception used to investigate an AI technique called Reinforcement Learning. In addition research will develop adversary simulator (in future years to be refined by computer network operations operator survey results). ***FY 2020 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
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 2018	FY 2019	FY 2020
ROLL CAGE will develop MTD and deception defense techniques based on game theoretic modeling to reflect realistic interactions of attackers and defenders. The research considers attack scenarios / patterns developed by an ally's Artificial Intelligence / Machine Learning (AI/ML) based intrusion detection simulator and tests the technologies using new attack patterns. The project will host a final demonstration. AIRS refines the reference architecture, ensuring that the system is able to understand and represent machine understandable languages. AIRS requires a high level understanding of machine understandable languages to make accurate system diagnoses. To ensure that the system has situational awareness, researchers will develop a representative simulation test environment with the requisite instrumentation to evaluate AIRS. Self-Securing Systems 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. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Additional resources will be used to complete development phase of projects under the Self-Securing Systems thrust.			
Title: Precise Cyber Effects ***Description:*** When compared to traditional methods of kinetic warfare, cyber conflicts are still relatively new and untested. Cyber operators often have incomplete information about their targets prior to completing an action. This deficit makes it difficult to predict the precise outcomes or collateral damage caused by a cyber operation. With this uncertainty, military leaders may act with an undue sense of caution in using cyber capabilities. Improving technology and techniques for quantifying cyber effects will increase the effectiveness of cost estimation, enhance consequence prediction and ensure precision. Highly precise and predictable cyber effects can also achieve mission goals despite the presence of both incomplete and maliciously-created false information. ***FY 2019 Plans:*** Identify and fund cyber seedling project(s) with potential impacts (intended and unintended) of employing cyber effects while limiting collateral damage. US-Australian bilateral Mission Assurance Research Collaboration (MARC) project arrangement will analyze data collected during TALISMAN SABRE (TS) 2017 command post exercise by applying mission mapping algorithms and machine learning processes. The algorithms, including identifying workflows, will characterize computing resources, and resolve individuals' identities across multiple modes of communication. The team will develop plans for strategic science and technology (S&T) inject into Pacific	3.235	3.340	3.387

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
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 2018	FY 2019	FY 2020
Sentry 2019 exercise. Researchers will identify use cases for validating dynamic mission mapping algorithms and processes through instrumentation of the field training exercise and command post exercise. ***FY 2020 Plans:*** MARC will curate and index data collected during the S&T inject of Pacific Sentry 2019 exercise. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Additional resources will be needed to further develop methods and tools for autonomous cyber operations.			
Title: Applied Mathematics for Cyber ***Description:*** Mathematics is intrinsically linked to all branches of science and technology, including cyber security research. 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. This area of research is needed to help characterize the cyber domain and cyber security, maintain the integrity of data, harden systems, and analyze potential solutions. Continued research in mathematical theory is crucial to maintain and increase the security of cyber systems. The goal of this effort is to provide the tools and techniques to improve the design and operation of cyber systems. ***FY 2019 Plans:*** "Stealthy Communications and Situational Awareness" project will initiate the integration of Linear Statistical Network Analysis (LSNA) matrix with the Naval Research Laboratory's Extensible Stealthy Protocol (NExtSteP) testbed to identify and classify channel embedding methods. In addition, research will also initiate production of high fidelity traffic using the NExtSteP testbed to analyze the types of channels that appear in candidate carrier protocols. "Mitigating Adversarial Machine Learning" (MAML) project will develop a prototype that simulates a framework for two- and three-model ensembles. The research composes models into ensembles to test for potential weaknesses and exploits within the overall system. ***FY 2020 Plans:*** The Stealthy project will continue to develop the LSNA infused NExtSteP testbed and determine whether metrics for "stealthiness" and throughput are consistent with the proof-of-concept overlay protocol. Research under the MAML project will investigate at least two evasion, inversion, and/or extraction attacks in a laboratory environment. The results will inform research on both ML model resilience and its effects on decision support and human operators. ***FY 2019 to FY 2020 Increase/Decrease Statement:***	1.965	2.023	2.053

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
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 2018	FY 2019	FY 2020
Additional resources are needed to complete the development phase of projects under the thrust.			
Accomplishments/Planned Programs Subtotals	14.429	14.935	15.118

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

- Number of publications in refereed journals and peer reviewed reports or conference proceedings;
- Number of external research collaborations and interactions with the broader cyber community;
- Transition of tools, techniques and methodologies for use in DoD, Federal or commercial entities;
- Improved technology readiness levels; and
- Affordability.