Exhibit R-2, **RDT&E Budget Item Justification:** PB 2019 Office of the Secretary Of Defense	**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
Total Program Element	-	11.906	14.775	14.969	-	14.969	15.162	15.443	15.712	16.010	Continuing	Continuing
003: *Cyber Applied Research*	-	11.906	14.775	14.969	-	14.969	15.162	15.443	15.712	16.010	Continuing	Continuing

Note

Service Requirements Review Board (SRRB) efficiencies are included.

A. Mission Description and Budget Item Justification

United States military forces require resilient and reliable networks, information, and weapons systems to conduct effective operations. However, the number and sophistication of threats in cyberspace are rapidly growing, making it critical to improve the cybersecurity of all Department of Defense (DoD) systems to counter those threats and assure the Department's missions. The Cyber Applied Research program focuses on innovative and sustained research in both cybersecurity and computer network operations to: develop new concepts to harden key network and computer components, design new and resilient cyber infrastructures, increase the military's ability to disrupt, fight and survive nation-state actors' cyber-attacks, measure the state of health in cybersecurity, and explore and exploit 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 targeted to meet Combatant Command 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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Previous President's Budget	12.183	14.775	15.075	-	15.075
Current President's Budget	11.906	14.775	14.969	-	14.969
Total Adjustments	-0.277	0.000	-0.106	-	-0.106
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.262	-			
• FFRDC Transfer	-0.013	-	-	-	-
• Other Program Adjustments	-0.002	-	-0.005	-	-0.005
• Economic Assumptiom	-	-	-0.101	-	-0.101

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2019 Office of the Secretary Of Defense	**Date:** February 2018
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*

Change Summary Explanation

FY 2019 adjustments are reflective of higher priority DoD requirements.

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
003: *Cyber Applied Research*	-	11.906	14.775	14.969	-	14.969	15.162	15.443	15.712	16.010	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Applied Research program was initiated in FY 2011 to address specific technical problems that were not being fully addressed by the Services' and the National Security Agency's existing Cyber science and technology (S&T) investments. Recently, S&T gaps were enumerated and described in several studies, including the 2015 DoD Cyber Strategy, the 2016 Commission Enhancing National Cybersecurity, and the 2017 Defense Science Board Research Enterprise Assessment.
The Cyber Applied Research program builds upon existing basic and applied research results. Over the past several years, the program expanded research in cyber capabilities to provide Warfighters and commanders with tools and technologies to enable cyber situational awareness, cyber command-and-control, cyber operations, and protection of tactical networks, weapons systems and platforms. From FY 2011 to FY 2017, the program explored a number of technical thrusts that included:

- Foundations of Trust: Developing known degrees of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error.

- Resilient Infrastructure: Exploring technologies that not only withstand, but react to cyber attacks, and sustain or recover critical functions.

- Assuring Effective Missions: Developing technologies that assess and control the cyber situation in mission context while staging, conducting, and monitoring cyber responses.

- Cyber Modeling, Simulation & Experimentation: Simulating environments in which the Department operates and enables a more robust assessment and validation of the cyber technology development.

- Embedded, Mobile & Tactical Environments: Exploring cyber systems that rely on technologies beyond wired networking and standard computing platforms.

As adversaries develop more sophisticated technology tactics and become more skilled and better funded, the Cyber S&T Community must remain agile, vigilant, and evermore creative in response. Starting in late FY 2016, the Department reviewed the emerging needs of the joint operational community, new cyber threats, and the evolution DoD technology needs to focus the program on the changing cyber environment and missions. To bolster this program and address future threats, a new strategic vision was developed to enhance the DoD's tactical edge in the rapidly evolving cyber domain where many aspects still remain unexplored. Seedling projects under the new research areas were initiated in late FY 2017. Judiciously investigating aspects of this research in thrusts areas identified below will provide a distinct advantage in future cyber conflicts:

- Behavioral Cyber Sciences: Exploring the interaction between computers and human behavior by moving beyond signals (ones and zeroes) towards understanding human behavior. New insights from behavioral sciences will increase the effectiveness of tools, the cyber workforce, and improve the utility of cyber solutions. Behavioral cyber sciences seeks to uncover details about how humans (to include 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 outcome.

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** 003 / *Cyber Applied Research*

• Self-securing weapons, systems, and networks: Prevailing in a contested cyber environment will require new sciences and mechanisms for autonomous cybersecurity to keep pace with the growing complexity of weapon systems and help the DoD operators react more quickly to cyber-attacks. Autonomous cyber defenses will need to apply the recent advances in artificial intelligence research.

• Foundations of precision cyber operations: Precision bombing campaigns for the cyber domain require accurate and timely predictions of cyber effects to enable DoD leadership to achieve the desired effects of cyber operations and help manage risks associated with collateral damage.

• Mathematical Foundations of Cyber Security: Advancing mathematical foundations of cyber S&T will cut across focus areas and produce new methods to design, secure, and reason about complex cyber systems.

Advances in these new cyber S&T focus thrust areas will help to promote strong foundations and disruptive innovations that will create surprises, shape the fight, and ensure a decisive advantage. The research areas will be critical to the development of innovative and sustainable research that takes cyber security beyond the incremental escalation of attack and defense.

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
Title: Foundations of Trust ***Description:*** Developed approaches and methods to establish known degrees of assurance that devices, networks, and cyber missions performed as expected, despite attack or error. This technical area encompassed all aspects of the assessment, establishment, propagation, maintenance, and composition of trust relationships between devices, networks, and people. Achieving a trustworthy cyberspace was a critical challenge as corporations, agencies, national infrastructure, and individuals have been victims of cyber-attacks, which exploit weaknesses in technical infrastructures as well as in human behavior. This effort built upon long term foundational basic research in algorithms, models, probability theory, reliability, statistical theory and analysis, system structures, and secure computing, developing and enabling trustworthy cyber systems. Research in algorithms helped develop methods to manipulate automated image processing computation using Scanning Electron Microscopes (SEMs), accelerating graphics processing unit (GPU) analysis. The development and compilation of GPU tools into a library provided meta-learning capabilities that were used to improve trust in digital electronics.	0.977	-	-
Title: Resilient Infrastructure ***Description:*** Resilient Infrastructure entailed the ability to withstand cyber attacks and to sustain or recover critical functions. This provided the ability to continue to perform functions and provided services at required levels during an attack. The objective in this area was to develop integrated architectures that were optimized for their ability to absorb cyber shock and recover in a timely fashion to a known secure state with well-defined performance characteristics. Resilient algorithms and protocols increased the repertoire of resiliency mechanisms available to the infrastructure and architecture. Research was needed to develop resiliency at lower levels with specific algorithms and protocols to support higher-level resilient architectures.	1.466	-	-

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
Funded research under the Tactical Platform Cyber Resiliency project, developed techniques for furnishing resiliency on critical real-time control systems against cyber-attacks. Through the enhancement of existing fault tolerance on physical systems, known as Byzantine Fault Tolerance (BFT), combinations of artificial, manipulated crashes, and delayed input evolved a level of tolerance to enforce resilience. The successful collaboration with Siemens transitioned the technology to the Naval Capability Program, Resilient Hull, Mechanical, and Electrical Security (RHIMES), which is now supports the NATO Sea Sparrow program. Under the Network PUMP-II project, research explored the challenges of optimizing enterprise based data sharing requirements for the tactical war-fighter and intelligence missions. The project developed a cost effective, high throughput government-off-the-shelf cross domain solutions that provided the war-fighter with improved sensitive data correlation and intelligent data decision capabilities. The technology is transitioning to the Naval Air Systems Command, Triton Unmanned Aircraft System Program Office.			
Title: Assuring Effective Missions ***Description:*** Assuring Effective Missions presented technology challenges in the areas of Cyber Mission Control and Effects at Scale. Within this thrust, research was developed to assess and control the cyber situation within a military mission context. Cyber Mission Control covered the ability to orchestrate cyber systems to achieve an overarching mission goal by developing tools and techniques that enabled models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain. Effects at Scale encompassed full spectrum challenges that intersected with cyber becoming a new full-fledged domain of warfare. Funded research under the Mission Assurance Research Collaboration (MARC), a U.S.-Australia cyber effort to enhance mission assurance through data enrichment, deep learning and natural language processing. The research developed dynamic mission mapping capabilities that were later integrated into Talisman Sabre 2017 (TS17). As a result, the MARC team successfully captured ~12 terabytes (TB) of operationally relevant, shareable data that it will use to analyze for future research. This massive data set represents a huge asset to the future of this five-year collaboration. Additionally, the team established relationships with I-CORPS and Deployable Joint Command and Control (DJC2) as the network providers for the exercise, laying the groundwork for capability demonstration, test, and evaluation in future exercises. ***FY 2018 Plans:*** MARC activities will focus on revising its mission assurance architecture and designing the MARC experiment for Talisman Saber 2019. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Research within this area will complete in FY 2018.	4.275	0.300	-
Title: Cyber Modeling, Simulation & Experimentation (MSE)	1.865	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
Description: Developed modeling and simulation capabilities that were able to sufficiently simulate the cyber environment in which the DoD operates and enables a more robust assessment and validation of cyber technology development. There were two technical challenges associated with cyber MSE: 1) Cyber Modeling and Simulation, and 2) Cyber Measurement. Cyber Modeling and Simulation sought to develop tools and techniques that enabled analytical modeling and multi-scale simulation of complex cyber systems. Cyber Measurement developed cyber experimentation and test range technology to conduct controlled, repeatable experiments, providing the ability to track the progress of cyber research investments in a quantitative fashion. This area explored new analytical methodologies, models, and experimental data sets to establish metrics to measure a system's state of security, applying the scientific method to establish the foundations of a framework in which cyber security research could be conducted, to test hypotheses with measurable and repeatable results, and the quantitative experimentation and assessment for new cyber technologies. These new methodologies enabled the exploration of modeling and simulation tools and techniques that drove innovation in research. Additionally, these methodologies aided in integrating experimentation by simulating the cyber environment with sufficient fidelity and integrating cyber modeling and simulation with the traditional modeling and simulation related to the kinetic domain. Funded research under the Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare (EW) and Communications/Networking project developed a selected set of vignettes and scenarios to understand the complex interactions between red and blue networks. The metrics derived from analyzing these scenarios were used to better inform future design choices in cyberspace, EW, and communications systems. The dynamic scenarios developed under this research are being migrated into to a distributed test-bed to support development of analytical tools.			
Title: Embedded, Mobile & Tactical Environments (EMT) ***Description:*** Increased the focus of cyber S&T on DoD cyber systems that relied on technology beyond wired networking and standard computing platforms. The objective in the area of embedded and tactical systems was to develop tools and techniques that assured the secure operation of microprocessors within our weapons systems and platforms; enabled security in real-time systems; and established security in disadvantaged, intermittent, and low-bandwidth environments. This research also sought to expand and cultivate military-grade techniques for securing and operating enterprise commodity mobile devices, such as smartphones, tablets, and their associated infrastructures. With the constant evolution of these devices and their respective infrastructures it was of the utmost importance to provide a secure environment where these devices could be effectively utilized, monitored and tracked. The Resilient and Assured Unmanned Aerial Systems Operations (RAUSO) project developed technologies to harden unmanned aerial systems (UAS) platforms and provided better cyber awareness to operators through the integration of a number of cyber tools and capabilities. The approach leveraged a high-assurance hardware platform developed under the Assured Resilient Embedded Systems (ARES) program, to build a cyber security module software stack capable of monitoring sensor inputs and	2.346	-	-

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019**
process behavior, while responding with security-relevant actions. The technology has been incorporated into the ARES platform and is being considered for a General Electric (GE) Aviation flight control system, with possible flight tests in FY 2018.			
Title: Behavioral Cyber Sciences ***Description:*** The point where hardware, software, and humans interact has become a jumping off point for a new area of research – behavioral cyber science. Cyber operations should be seen in the context of a larger socio-behavioral-technical domain. Research in behavioral cyber science seeks to advance the understanding and technical rigor of modeling and predicting human responses to cyber activities and to discover ways to inject this understanding into the human aspects of cyber operations, cyber defense systems, planning, and training. Future research must broaden the scope beyond the impacts of cyber actions on equipment, and also include the impact that these cyber actions will have on broader human behavior. Just as an adversary's behavior may be better understood using behavioral cyber science, behavioral science can be utilized to help understand ways 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 cyber workforce design better techniques and processes for use in cyber defense. ***FY 2018 Plans:*** Begin execution of Joint research effort aimed at addressing scientific challenges, to broaden the scope of cyber activities through an understanding of human behavioral sciences and its responses to cyber effects. Research will focus on human performance for cyber, developing techniques to measure effectiveness of cyber tools and cyber mission planning based on behavior of network defenders; human responses to cyber effects, identifying and documenting human responses to cyber defense and offense activities; and evidence-based validation, which identifies behavioral responses to network activity that correlate with information on network security and readiness. ***FY 2019 Plans:*** Continue the development of behavioral cyber science research with follow-on efforts from early FY 2017 and FY 2018 with a large scale study to derive statistically-relevant results. Incorporate insights into research prototypes to analyze early results in mission-simulated settings. Codify sound methodological approaches to accurately address cyber challenges that identify communities of risk; improve efficiency/effectiveness of cyber teams to cyber-attack; and research the impact of social engineering as a major vulnerability. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Additional resources will allow for completion of the development phase of the projects under the thrust.	0.391	3.700	3.774
Title: Self-securing Weapons, Systems, and Networks ***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.	-	5.775	5.788

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
Software can often be disrupted remotely, which necessitates a new kind of security to protect against 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. The Department can expect future cyber adversaries to be well-funded, well-informed, and agile. Building weapon systems, platforms, and networks that can defend themselves in real time will be vital in protecting ourselves against the adversary. The DoD needs systems that will autonomously monitor and manage their own health and security posture through advanced sensing and perception, reasoning, and planning. Such systems could identify and classify threats much more quickly than a human operator, and therefore, be able to 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 is crucial to ensure that direct control can be reasserted, potentially reversing actions, if necessary. ***FY 2018 Plans:*** Begin execution of Joint research effort aimed at developing novel adaptive techniques to model adversary options and predict the security of future system configurations, even under unknown attacks; develop cyber immunology so that systems can monitor health and develop identification/classification mechanisms for cyber threats; develop autonomy methods and self-healing techniques couple with rigorous experimentation; develop experimental approaches to prove robust and unique metrics; and use advanced modeling and simulation to develop and validate cyber security metrics. ***FY 2019 Plans:*** Continue developing novel adaptive techniques that focus on a system's ability to reason about its own security and take action without immediate human inputs; explore self-healing techniques associated with Internet of Things (IoT) devices with largely unattended sensing, computation, storage, and heavy machine-to-machine (M2M) communication. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase will allow the program to complete the development phase of projects under the thrust.			
Title: Foundations of Precision Cyber Operations ***Description:*** When compared to traditional methods of kinetic warfare, cyber conflict is still relatively new and untested. Cyber operators often have incomplete information about their target prior to completing an action. The lack of a complete picture makes it difficult to predict the precise outcomes or collateral damage caused by a cyber operation. In this type of uncertain environment, military leaders may be acting with an undue sense of caution in using cyber capabilities. Improved technology and techniques for quantifying cyber effects, estimating their cost and effectiveness, predicting consequences, and ensuring precise effects will help both to limit collateral damage and to ensure that a chosen action has the intended effect upon the adversary. Highly precise and	0.586	3.000	3.367

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
predictable cyber effects can also achieve mission goals despite the presence of both incomplete and maliciously-created false information. ***FY 2018 Plans:*** Begin execution of Joint research effort aimed at developing greater precision and accuracy of cyber effects to achieve targeted cyber mission impacts. Research will focus on developing modeling techniques, based on limited data, capable of predicting the range of possibilities that unfold due to a planned cyber effect; developing methods to collect technical information from inaccessible cyber systems, while employing covert deceptive techniques; developing methods to identify key pieces of missing information to advance situational awareness; developing abductive reasoning techniques; developing intelligent systems that can reason and provide actionable guidance despite the presence of both incomplete and maliciously-created false information; developing methods for autonomous cyber operations to provide enhanced control and execution that allow cyber operators to timely and accurately respond to events. ***FY 2019 Plans:*** Continue research in modeling techniques that support effects planning, and its ability to characterize systems, networks, devices, and software from a distance. The ability to establish a course of action before an effect is deployed is critical to its use, developing methods to collect technical information from inaccessible cyber systems, while employing covert deceptive techniques; will develop methods to identify key pieces of missing information to advance situational awareness. Will Identify rapid methods to developing actionable guidance despite incomplete information. Will develop methods for autonomous cyber operations to provide enhanced control and execution that allow cyber operators to timely and accurately respond to events. MARC activities will focus on developing and refining tools to incorporate into its mission assurance architecture and designing the MARC experiment for Talisman Sabre 2019 Exercises. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase will allow the program to further develop methods and tools for autonomous cyber operations.			
Title: Mathematical Foundations of Cyber Security ***Description:*** Mathematical Foundations of Cyber Security 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 beyond the “basic research” level is crucial to maintain and increase the security of cyber systems. Mathematics is intrinsically linked to all branches of science and technology including cyber security research. There is a need for an array of modeling techniques, both informal and formal, backed by various rigorous mathematical theories, to capture and support the richness of the cyber domain. ***FY 2018 Plans:***	-	2.000	2.040

Exhibit R-2A, **RDT&E Project Justification:** PB 2019 Office of the Secretary Of Defense		**Date:** February 2018
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 2017**	**FY 2018**	**FY 2019**
Execution of a Joint research effort aimed at developing and enhancing foundational work underpinning cyber technology in the areas of advanced mathematics. Possible research areas include mathematical logic and formal methods; network science; information theory; decision sciences; risk analysis; and modeling and simulation. ***FY 2019 Plans:*** Development of research areas under mathematical logic and formal methods, where modeling techniques identify salient features satisfied by systems. Research will investigate the capacity of overt and covert channels in an effort to address cyber security challenges using information theory to provide rigorous interpretations of a machine’s channel capacities. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The FY 2019 increase will allow the program to complete the development phase of projects under the thrust.			
Accomplishments/Planned Programs Subtotals	11.906	14.775	14.969

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.