Exhibit R-2, **RDT&E Budget Item Justification:** FY 2018 Office of the Secretary Of Defense	**Date:** May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
Total Program Element	-	15.378	12.183	14.775	-	14.775	15.075	15.249	15.552	15.877	Continuing	Continuing
P003: *Cyber Applied Research*	-	15.378	12.183	14.775	-	14.775	15.075	15.249	15.552	15.877	Continuing	Continuing

A. Mission Description and Budget Item Justification

Our 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 cyber security of all Department of Defense (DoD) systems to counter those threats and assure our missions. The Cyber Applied Research program focuses on innovative and sustained research in both cyber security 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 cyber security, 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 (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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	13.701	12.183	15.043	-	15.043
Current President's Budget	15.378	12.183	14.775	-	14.775
Total Adjustments	1.677	0.000	-0.268	-	-0.268
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	1.923	-			
• SBIR/STTR Transfer	-0.246	-			
• Other Adjustments	-	-	-0.268	-	-0.268

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense			**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
P003: *Cyber Applied Research*	-	15.378	12.183	14.775	-	14.775	15.075	15.249	15.552	15.877	Continuing	Continuing

A. Mission Description and Budget Item Justification

This program was initiated in FY 2011 to address specific technical problems that were not being fully addressed by the Services' and NSA's existing Cyber 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. The program expands research in cyber command-and-control to provide Warfighters and commanders with tools and technologies to enable cyber situational awareness and protection of tactical networks, weapons systems and platforms. Current technical thrusts include: Foundations of Trust, Resilient Infrastructure, Assuring Effective Missions, Cyber Modeling, Simulation & Experimentation, and Embedded, Mobile & Tactical Environments.

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. To bolster this program and address future threats, starting in FY 2017 a new strategic vision was directed at enhancing the DoD's tactical edge in the rapidly evolving cyber domain where many aspects still remain unexplored. Judiciously investigating these aspects by investing in the research thrust areas identified below can provide a distinct advantage in future cyber conflicts:

- Behavioral Cyber Sciences: The interaction between computers and human behavior. 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 cyber solutions at DoD scale. 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.

- Self-securing weapons, systems, and networks: Thriving in a contested cyber environment. New sciences and mechanisms for autonomous cybersecurity will help keep pace with the growing complexity of weapon systems and help the DoD operators react more quickly to cyber-attacks.

- Foundations of precision cyber operations: Precision bombing campaigns for the cyber domain. Accurate and timely predictions of cyber effects will help the DoD leadership achieve the desired effects of cyber operations and help manage risks associated with collateral damage.

- Mathematical Foundations of Cyber Security: New tools to address new problems. Advances in 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.

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
Title: Foundations of Trust ***Description:*** Develop approaches and methods to establish known degrees of assurance that devices, networks, and cyber missions perform as expected, despite attack or error. This technical area encompasses all aspects of the assessment, establishment, propagation, maintenance, and composition of trust relationships between devices, networks, and people. Achieving a trustworthy cyberspace is 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 builds 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. ***FY 2016 Accomplishments:*** This program funded research on “Scanning Electron Microscope (SEM) Image Processing” to improve image processing computation by identifying and categorizing steps to improve Graphics Processing Unit (GPU) acceleration to improve our trust in digital electronics. This effort completed the compilation of a library of GPU tools. “Pointillist” a project executed by John Hopkins University Applied Physics Laboratory (JHU/APL), developed a graph analytic engine to monitor network traffic in real-time. The features of Pointillist allow hunt teams to visualize and identify adversarial network traffic faster. The work developed an infrastructure that tailored user interfaces with automated software-driven processes and supported easy configuration of incoming data streams. The interactive visualization tool improved interoperability to increase ease-of-adoption and decrease training time for analysts working on specialized missions such as Cyber Protection Team Hunt sub-teams. This helped improve trust and provide real-time situational awareness (SA) of cyber enabled assets. ***FY 2017 Plans:*** Complete research on the “SEM Image Processing” effort’s improved automated image processing technology by developing algorithms and methods to accelerate GPU analysis. The research focuses on developing sets of advanced modules via a process called fusion that enhances capabilities of a meta-learning framework. Fusion combines many data structure extractors into one structure extractor.	1.563	1.000	-
Title: Resilient Infrastructure ***Description:*** Resilient Infrastructure entails the ability to withstand cyber attacks, and to sustain or recover critical functions. This provides the ability to continue to perform functions and provide services at required levels during an attack. The objective in this area is to develop integrated architectures that are 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 increase the repertoire of resiliency mechanisms available to the infrastructure and architecture. Research is needed to develop resiliency at lower levels with specific algorithms and protocols to support higher-level resilient architectures.	1.055	1.500	-

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**

FY 2016 Accomplishments:

The "Network Pump-II" project, executed by Naval Research Laboratory (NRL), 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 solution that was demonstrated at various venues including the Universal Gateway (UGW)/Pump-II Limited Technology Experiment. The impact of research under "Pump-II" provided the war-fighter with improved sensitive data correlation and intelligent data decision capabilities. A number of transitions are under way with the Naval Air Systems Command, Triton Unmanned Aircraft System Program Office for Pump-II with Secret and Below Interoperability certification and the Office of Naval Research Integrated Topside and Multi-Link Common Data Link System with Top Secret and Below Interoperability certifications.

The "Tactical Platform Resiliency" project executed by the Office of Naval Research (ONR) improved the design and robustness of various fault tolerant tools used to harden critical control systems. The effort also designed and developed capabilities to monitor and autonomously remove malicious code and commands and data from compromised networks.

The "Control Flow Integrity Monitoring" project executed by JHU/APL developed methods of detecting "return-oriented" programming attacks using record-and-replay technology. This technology enabled the rapid detection of some zero-day attacks that otherwise bypass all modern defenses. This eliminated the effectiveness of a large class of exploits.

A second JHU/APL executed project, "System Cloaking Defense through Deception," demonstrated ways to present decoys to adversaries and detect their presence and activities. A major impact of the project raised attacker workloads, confused, delayed, and disrupted an adversary's ability to execute exploitation operations. System cloaking is being considered for transition to a number of organizations namely ONR, Army Cyber (ARCYBER), Marine Force Cyber (MARFORCYBER) and Department of Homeland Security (DHS).

FY 2017 Plans:

In FY 2017, ONR efforts under the "Tactical Platform Resiliency" project will develop methods and techniques for furnishing resiliency on critical real-time control systems against cyber-attacks. Additionally, ONR will experiment with and evaluate resilience techniques through its Small Business Innovative Research (SBIR) performers. Projects that were designed to quickly transition to operational partners will continue maturing capabilities, inhibiting advanced threats, improving technology maturity, and exploring transition opportunities.

Title: Assuring Effective Missions	5.000	4.375	0.300

Description: The objective of Assuring Effective Missions presents technology challenges in the areas of Cyber Mission Control and Effects at Scale. Within this thrust, we aim to develop the ability to assess and control the cyber situation within a military mission context. Cyber Mission Control covers the ability to orchestrate cyber systems to achieve an overarching mission goal by

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)

developing tools and techniques that enable models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain. Effects at Scale encompass full spectrum challenges that intersect with cyber becoming a new full-fledged domain of warfare.

This program funds an international research collaboration effort under the Mission Assurance Research Collaboration (MARC) project arrangement. The overall research focus of MARC is to enhance mission assurance through data enrichment, deep learning and natural language processing. MARC aims to provide dynamic mission mapping capability by enabling the timely identification and characterization of cyber terrain, missions and their interdependencies.

FY 2016 Accomplishments:
This program funded a project led by the U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) called “Defensible Offensive Cyber Operations (OCO) Architecture and Cyber Situational Awareness”, which developed a cross-service cloud-based defense architecture system that allows the sharing of SA capabilities to enable near-real time decision making and battle damage assessment. The interoperable reference architecture provides an ability to detect, maneuver and restore impacted capabilities “to survive and operate through the fight” for existing and future OCO architectures. Additionally, the OCO architecture supports USCYBERCOMMAND’s priority number one and two gaps for cyber infrastructure defense and SA.

The Mission Assurance Research Collaboration (MARC) program arrangement was formally initiated as a bilateral research effort between the U.S. and Australia. Program planning and experimental design was completed during this fiscal year. Additionally, the research team made improvements to the mission mapping algorithm and established a bilateral collaborative environment.

FY 2017 Plans:
During FY 2017, the “Defensible OCO Architecture and Cyber Situational Awareness” project will test the prototype cloud-based defense architecture. Upon successful completion of testing, the existing cyber situational awareness tools will be integrated and implemented into the OCO architecture.

MARC will aim to complete instrumentation during TALISMAN SABER 17 exercises. Additional research objectives include proof-of-concept and testing of a machine finger-printing algorithm. Final research papers on deep learning, natural language processing, entity extraction/characterization and workflow discovery will also be produced.

FY 2018 Plans:
MARC activities will focus on revising its mission assurance architecture and designing the MARC experiment for TALISMAN SABER 19.

	FY 2016	**FY 2017**	**FY 2018**
Title: Cyber Modeling, Simulation & Experimentation (MSE)	2.360	1.908	-

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
Description: Develop modeling and simulation capabilities that are able to sufficiently simulate the cyber environment in which the DoD operates and enable a more robust assessment and validation of cyber technology development. There are two technical challenges associated with cyber MSE: 1) Cyber Modeling and Simulation, and 2) Cyber Measurement. Cyber Modeling and Simulation seeks to develop tools and techniques that enable analytical modeling and multi-scale simulation of complex cyber systems. Cyber Measurement develops 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 explores new analytical methodologies, models, and experimental data sets to establish metrics to measure a system's state of security, apply the scientific method to establish the foundations of a framework in which cyber security research can be conducted, to test hypotheses with measurable and repeatable results, and the quantitative experimentation and assessment for new cyber technologies. These new methodologies will enable the exploration of modeling and simulation tools and techniques that can drive innovation in research. Additionally, these methodologies will aid in integrated 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. ***FY 2016 Accomplishments:*** In FY 2016, the "Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare (EW) and Communications/Networking" developed a selected set of vignettes and scenarios to understand the complex interactions between red and blue networks and to derive metrics that can be used to design better cyberspace, EW, and communications systems in support of information dominance. The performer successfully integrated Cyber, EW, and Communications/ Networking into a common test environment that was based on well-defined vignettes. From this scenario, metrics were developed that accurately evaluated the performance of Cyber, EW and communications in an anti-access area denial (A2AD) environment. ***FY 2017 Plans:*** The "Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare and Communications/Networking" project will develop and fine-tune joint metrics that will be utilized in dynamic and causal workflows. The dynamic scenarios will be used to migrate to a distributed test-bed to support more nodes and the development of analytical tools.			
Title: Embedded, Mobile & Tactical Environments (EMT) ***Description:*** Increase the focus of cyber S&T on DoD cyber systems that rely on technology beyond wired networking and standard computing platforms. The objective in the area of embedded and tactical systems is to develop tools and techniques that assure the secure operation of microprocessors within our weapons systems and platforms; enable security in real-time systems; and establish security in disadvantaged, intermittent, and low-bandwidth environments. This research also seeks 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	5.400	2.400	-

<u>**B. Accomplishments/Planned Programs ($ in Millions)**</u>	**FY 2016**	**FY 2017**	**FY 2018**
infrastructures it is of the utmost importance to provide a secure environment where these devices can be effectively utilized, monitored and tracked. ***FY 2016 Accomplishments:*** In FY 2016, the "Resilient and Assured Unmanned Aerial System (UAS) Systems and Operations" project identified and improved APTs sensing technologies, increasing overall avionics system cyber resiliency. These characteristics helped researchers develop techniques to mitigate mission-deviant behavior directed by APTs. The enhanced capabilities provided operators/mission commanders with previously unavailable near real-time actionable, clear and useful cyber dependent information. The project has demonstrated proof-of-concept technologies that provide situational awareness of the platform's cyber health to UAS pilots/ operators and mission commanders. ***FY 2017 Plans:*** The "Resilient and Assured UAS and Operations" project effort during FY 2017 will demonstrate the prototype mission computer that will encompass technologies developed in prior years. The Testbed for Resilient UAS Engineering will undergo refinement and an assessment of attestation techniques. A joint DARPA/AFRL demonstration is in the planning stage. Potential transition opportunities include Air Force Life Cycle Management Center, NRL, Naval Air Systems Command, and CERDEC for experimentation.			
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 2017 Plans:*** Plan for a new research effort under Behavioral Cyber Sciences that will identify and validate the proposed hypotheses. Research will identify sensor data that correlates strongly to human responses. ***FY 2018 Plans:***	-	0.400	3.700

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
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.			
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. 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. We 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 this adversary. We need systems that can 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, 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 some 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.	-	-	5.775
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	-	0.600	3.000

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
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 predictable cyber effects can also achieve mission goals despite the presence of both incomplete and maliciously-created false information. ***FY 2017 Plans:*** Plan for a new research effort under Foundations of Precision Cyber Operations that will improve accuracy and precision of cyber effects to achieve cyber mission impacts comparable to precision bombing campaigns for the cyber domain. Initiate research efforts to develop techniques and methods to build stealthy protocols and develop high fidelity models of industrial control systems capable of rapidly representing realistic responses at the physical layer as events occur. ***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 in-accessible 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.			
Title: Mathematical Foundations of Cyber Security ***Description:*** Mathematics is intrinsically linked to all branches of science and technology. Cyber security research is no exception. Broadly, 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. 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 beyond the “basic research” level is crucial to maintain and increase the security of cyber systems. ***FY 2018 Plans:*** This funds the execution of 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.	-	-	2.000
Accomplishments/Planned Programs Subtotals	15.378	12.183	14.775

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z **/** *Cyber Security Research*	**Project (Number/Name)** P003 **/** *Cyber Applied Research*

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
- Affordability