Exhibit R-2, **RDT&E Budget Item Justification:** PB 2016 Office of the Secretary Of Defense	**Date:** February 2015
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* **/** BA 3: *Advanced Technology Development (ATD)*	**R-1 Program Element (Number/Name)** PE 0603668D8Z **/** *Cyber Security Advanced Research*

COST ($ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
Total Program Element	-	11.150	-	-	-	-	-	-	-	-	Continuing	Continuing
P113: *Cyber Advanced Technology Development*	-	11.150	-	-	-	-	-	-	-	-	Continuing	Continuing

A. Mission Description and Budget Item Justification

Our military forces require resilient, reliable networks and computer 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 DoD networks to counter those threats and assure our missions. This program focuses on innovative and sustained advanced development in both cyber security and computer network operations to mature new concepts to harden key network and computer components to include: designing new resilient cyber infrastructures; increasing the military's ability to fight and survive during cyber attacks; disrupting nation-state level attack planning and execution; measuring the state of cyber security for the U.S. government; increasing our understanding of cyber as a war-fighting domain; and providing modeling and simulation of cyberspace operations to explore and exploit new ideas in cyber warfare for agile cyber operations and mission assurance, and protection of tactical networks, weapons systems and platforms.

The Cyber Advanced Technology Development program element (PE) was budgeted in the advanced technology development budget activity because it focused on the maturation of successful applied research results, and their development, into demonstrable advanced cyber security capabilities. The Cyber Advanced Technology Development program built upon the results of matured applied research from the Cyber Applied Research PE (0602668D8Z), and other programs, to develop technology demonstrations for potential transition into capabilities that support the full spectrum of computer network operations. These approaches included moving from cyber defense to cyber resilience by changing the defensive terrain of our existing digital infrastructure, identifying ways to raise the risk and lower the value of an attack from an advanced persistent cyber threat, and focusing on mission assurance metrics.

The program focused on science & technology (S&T) to address joint problems in cyber defense and operations. The focus of the research was on filling capability and technology gaps identified in the Cyber Community of Interest S&T Roadmap, the 2013 Cyber S&T Capability Gap Framework and other assessments conducted by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)).

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2016 Office of the Secretary Of Defense	**Date:** February 2015
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 3: *Advanced Technology Development (ATD)*	**R-1 Program Element (Number/Name)** PE 0603668D8Z / *Cyber Security Advanced Research*

B. Program Change Summary ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Previous President's Budget	9.667	-	-	-	-
Current President's Budget	11.150	-	-	-	-
Total Adjustments	1.483	-	-	-	-
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	1.795	-			
• SBIR/STTR Transfer	-0.312	-			

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense		**Date:** February 2015
Appropriation/Budget Activity 0400 **/** 3	**R-1 Program Element (Number/Name)** PE 0603668D8Z **/** *Cyber Security Advanced Research*	**Project (Number/Name)** P113 **/** *Cyber Advanced Technology Development*

COST ($ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
P113: *Cyber Advanced Technology Development*	-	11.150	-	-	-	-	-	-	-	-	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Advanced Technology Development program built upon, matured, and transitioned the results of successful applied research results from the Cyber Applied Research PE. The link between the Cyber Applied Research and Cyber Advanced Technology Development PEs was intended to create a mechanism to take existing basic research results and mature them to the point of incorporation into technology demonstrations. This program focused on science & technology (S&T) to address joint challenges in cyber defense and operations. The focus of the research was on filling capability and technology gaps identified in the Cyber Community of Interest S&T Roadmap, the 2013 Cyber S&T Capability Gap Framework and other assessments conducted by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)). Progress and results are reviewed by the Cyber S&T Community of Interest.

Beginning in FY 2013, the program expanded research in cyber command and control to provide warfighters and commanders new situational awareness, course of action analysis, cyber operational agility and cyber mission control. This research included protection of tactical networks, weapons systems and platforms. The six new technical thrust areas were:

Foundations of Trust
Resilient Infrastructure
Agile Operations
Assuring Effective Missions
Cyber Modeling, Simulation, and Experimentation (MSE)
Embedded, Mobile, and Tactical Environments (EMT)

B. Accomplishments/Planned Programs ($ in Millions)	FY 2014	FY 2015	FY 2016
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. ***FY 2014 Accomplishments:*** - Extended host integrity measurement and checking to cloud and virtualized platforms. - Implemented trust-based approaches to computer network defense.	4.815	-	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense		**Date:** February 2015
Appropriation/Budget Activity 0400 **/** 3	**R-1 Program Element (Number/Name)** PE 0603668D8Z **/** *Cyber Security Advanced Research*	**Project (Number/Name)** P113 **/** *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016**
- Modeled and analyzed composite trust management schemes that provide increased ability to assess the trustworthiness of complex interconnected systems and software.			
Title: Resilient Infrastructure ***Description:*** Entails the ability to withstand cyber attacks, and to sustain or recover critical functions. A resilient infrastructure has the ability to continue to perform its functions and provide its 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 address novel protocols and algorithms to 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. ***FY 2014 Accomplishments:*** - Developed methods for increasing resilience of operational systems. - Developed mechanisms to compose resilient systems from brittle components.	1.482	-	-
Title: Assuring Effective Missions ***Description:*** Develop the ability to assess and control the cyber situation within a military mission context. While the focus in cyber research is often placed on individual technologies, how these technologies work toward an effective mission is critical for the DoD. The objective of Assuring Effective Missions presents technology challenges in the areas of Cyber Mission Control and Effects at Scale. Cyber Mission Control covers the ability to orchestrate cyber systems to achieve an overarching mission goal. To perform dynamic analysis of asset criticality and course of action analysis alternatives, there is a critical need for tools that can map information technology assets to missions and use modeling and simulation, or other techniques. Inherent in Cyber Mission Control is the ability to automatically derive and fuse information about the characteristics of information technology systems in a manner that allows us to describe, analyze, observe, and control the operation of information technology components. A key goal of this research area is to have tools that enable commanders to assess and direct different information technology maneuvers in conjunction with mission actions. Effects at Scale encompass full spectrum challenges that intersect with cyber becoming a new full-fledged domain of warfare. ***FY 2014 Accomplishments:*** - Developed foundational cyber interoperability framework to enable rapid integration and reduced acquisition and integration cost for the development of current and future cyber mission operations.	0.730	-	-
Title: Cyber Modeling, Simulation & Experimentation (MSE)	1.618	-	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense		**Date:** February 2015
Appropriation/Budget Activity 0400 **/** 3	**R-1 Program Element (Number/Name)** PE 0603668D8Z **/** *Cyber Security Advanced Research*	**Project (Number/Name)** P113 **/** *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016**
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 modeling, simulation, and experimentation: 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 will explore 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 2014 Accomplishments:*** - Developed approaches and tools to incorporate cyber models into mission, physical and kinetic simulations to achieve increased fidelity and coverage. - Developed cyber simulation models that incorporate mission models and cyber-kinetic effects.			
Title: Embedded, Mobile & Tactical (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 platforms and systems; 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 with enterprise-style commodity mobile devices, such as smartphones, tablets, and their associated infrastructures. With the constant evolution of these devices and their respective infrastructures it is of the utmost importance to provide a secure environment where these devices can be effectively utilized, monitored and tracked. ***FY 2014 Accomplishments:*** - Developed efficient algorithms capable of locating and tracking stationary and mobile emitters to help protect DoD networks from wireless intrusion.	2.505	-	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense	**Date:** February 2015

Appropriation/Budget Activity 0400 **/** 3	**R-1 Program Element (Number/Name)** PE 0603668D8Z **/** *Cyber Security Advanced Research*	**Project (Number/Name)** P113 **/** *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016**
- Developed and tested hardware capable of rapidly providing accurate line of bearing to wireless emitters.			
Accomplishments/Planned Programs Subtotals	11.150	-	-

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• BA 2, PE # 0602668D8Z, P003: *Cyber Applied Research*	11.637	14.979	13.727	-	13.727	12.966	15.249	15.537	15.748	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A