Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense											Date: March 2014	
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 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
Total Program Element	-	10.542	13.907	15.000	-	15.000	15.285	15.575	15.871	16.173	Continuing	Continuing
P003: *Cyber Applied Research*	-	10.542	13.907	15.000	-	15.000	15.285	15.575	15.871	16.173	Continuing	Continuing

The FY 2015 OCO Request will be submitted at a later date.

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 urgent and critical to improve the cyber security of 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 resilient cyber infrastructures, increase the military's ability to fight and survive during cyber attacks, disrupt nation-state level attack planning and execution, measure the state of cyber security, and explore and exploit new ideas in cyber warfare for agile cyber operations and mission assurance.

This program builds upon existing basic and applied research results. The program focuses on integrating computer network defense and computer network operations, addressing joint problems in cyber operations, and filling capability and technology gaps as identified in the 2012 Cyber Priority Steering Council Science and Technology Roadmap and 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 DoD Cyber Science & Technology Community of Interest. New efforts will also be aligned with emerging U.S. Cyber Command Mission Requirements.

B. Program Change Summary ($ in Millions)	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO**	**FY 2015 Total**
Previous President's Budget	18.985	18.908	23.675	-	23.675
Current President's Budget	10.542	13.907	15.000	-	15.000
Total Adjustments	-8.443	-5.001	-8.675	-	-8.675
• Congressional General Reductions	-7.500	-5.000			
• Congressional Directed Reductions	-0.948	-			
• Congressional Rescissions	-0.015	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	0.291	-			
• SBIR/STTR Transfer	-0.267	-			
• FFRDC Adjustment	-	-0.001	-	-	-
• Other Program Adjustments	-0.004	-	-	-	-
• Strategic Efficiency Savings	-	-	-8.675	-	-8.675

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602668D8Z *I Cyber Security Research*

Change Summary Explanation

The reduction is a strategic efficiency approach to reduce funding and staffing. As a result, we provide a better alignment of funding and provide support to a smaller military force.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense			Date: March 2014
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 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
P003: *Cyber Applied Research*	-	10.542	13.907	15.000	-	15.000	15.285	15.575	15.871	16.173	Continuing	Continuing

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

This program builds upon existing basic and applied research results. The program focuses on integrating computer network defense and computer network operations, addressing joint problems in cyber operations, and filling capability and technology gaps as identified in the 2012 Cyber Priority Steering Council Science and Technology Roadmap and 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 DoD Cyber Science & Technology 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 will include protection of tactical networks, weapons systems and platforms. Beginning in FY14, new efforts will also be aligned with emerging U.S. Cyber Command Mission Requirements.

The six technical thrust areas include:

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 2013	FY 2014	FY 2015
Title: Foundations of Trust	1.055	1.390	1.500
Description: Develop approaches and methods to establish known degree of assurance that devices, networks, and cyber dependent functions 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 2013 Accomplishments: - Developed scalable reverse engineering and analysis toolset.			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense		Date: March 2014
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 2013	FY 2014	FY 2015
- Created cost-effective technology for the construction of high-assurance cyber-physical systems, meaning functionally correct and satisfying appropriate safety and security properties. ***FY 2014 Plans:*** - Explore and identify trust establishment, propagation, and maintenance techniques. - Develop trustworthy architectures and trust composition tools. - Develop interfaces to the reverse toolset and code libraries. - Develop test tool for multiple systems architectures. ***FY 2015 Plans:*** - Develop a non-signature based capability to detect malicious code on cyber systems with high accuracy. - Develop trustworthy architectures and trust composition tools. - Detection algorithms for malicious USB firmware/hardware.			
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, even if this is at the expense of degraded performance. 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 resilience at lower levels with specific algorithms and protocols to support higher-level resiliency architectures. ***FY 2013 Accomplishments:*** - Developed analytical model for routing techniques in the presence of jamming. - Understood new mechanisms for secure operation of many-core chips. - Identified mechanisms to compose resilient systems from brittle components. - Monitored, protected and reconfigured a host system or peripheral components that are targeted during an attack. ***FY 2014 Plans:*** - Develop methods for increasing resiliency of operational systems. - Integrate sensing, detection, response, and recovery mechanisms. - Design framework for secure modularization and virtualization of nodes and networks. - Develop advanced Computer Network Defense (CND) components and management features for the CND framework. - Develop methods for increasing resiliency of large scale tactical networks while introducing increased mobility. - Conduct resiliency-specific modeling and simulation.	4.217	5.563	1.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense		Date: March 2014
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 2013	FY 2014	FY 2015
- Develop code-level software resiliency. ***FY 2015 Plans:*** - Conduct spectral analysis of Random Matrix Theory to extend beyond origination destination. - Explore learning algorithms to distinguish abnormal traffic patterns from normal traffic patterns.			
Title: Agile Operations ***Description:*** Explore new methods and technologies to dynamically reshape cyber systems as conditions/goals change, to escape harm, or to manipulate the adversary. These capabilities present technology challenges in the areas of Autonomic Cyber Agility and Cyber Maneuver. Cyber Maneuver is a new way to manage systems dynamically in a cyber situation. It is a set of emerging methods for maintaining defensive or offensive advantage in cyber operations. It entails developing mechanisms that enable goal-directed reshaping of cyber systems. Cyber maneuver encompasses reallocation for repurposing a device or platform, reconfiguration for changing the way a system performs a task, and repositories for altering the operating state in a logical or physical topology. Autonomic Cyber Agility covers several forms of agility. As cyber infrastructures increase in scale and complexity, there is an urgent need for autonomous and agile mechanisms to reconfigure, heal, optimize, and protect defensive and offensive cyber mechanisms. ***FY 2013 Accomplishments:*** - Researched and analyzed the security architectures of various major web engines such as Trident and Gecko. - Designed distributed systems architectures and service application polymorphism. - Transitioned ARCSYNE from Internet Protocol version (IPV) 4 to IPv6. ***FY 2014 Plans:*** - Design distributed systems architectures and service application polymorphism. - Develop machine intelligence techniques for autonomous reprogramming, reconfiguration, and control of cyber components ***FY 2015 Plans:*** - Design distributed systems architectures and service application polymorphism. - Develop techniques for autonomous reprogramming, reconfiguration, and control of cyber components, and machine intelligence. - Develop automated reasoning techniques for executing courses of action.	3.162	2.086	2.000
Title: Assuring Effective Missions ***Description:*** Develop the ability to assess and control the cyber situation in the 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.	2.108	1.391	3.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense		Date: March 2014
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 2013	FY 2014	FY 2015
To perform dyanmic 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 2013 Accomplishments:*** - Researched trusted information flow architectures, frameworks, and mechanisms for application to tactical assured information sharing environments. - Developed techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure. - Developed techniques for course of action development and analysis. - Improved realism through automated mission modeling and mission situational awareness. ***FY 2014 Plans:*** - Enable cyber effects assessment. - Automate mapping of mission essential functions – cyber resources using multi-attribute identifiers. - Identify critical assets and potential rogue workflows. - Develop metrics with which the DoD could maintain Computer Network Defense (CND) capabilities to thwart certain classes of APTs and other threats. ***FY 2015 Plans:*** - Assess effectiveness of agility mechanisms and moving target techniques against Advanced Persistent Threats (APT). - Develop metrics with which the DoD could maintain Computer Network Defense (CND) capabilities to thwart certain classes of APTs and other threats. - Design distributed systems architectures and service application polymorphism.			
Title: Cyber Modeling, Simulation & Experimentation (MSE) ***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	-	1.391	3.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense		Date: March 2014
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 2013	FY 2014	FY 2015
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 hypothesis with measurable and repeatable results, and the quantitative experimentation and assessment for new cyber technologies. These new methodologies will enable exploration of modeling and simulation tools and techniques that can drive innovation in research and aid in integrated experimentation and transition to operations to simulate the cyber environment with sufficient fidelity, and to integrate cyber modeling and simulation with the traditional modeling and simulation related to the kinetic domain. ***FY 2014 Plans:*** - Develop methods to plan and execute large-scale cyber engagements. - Conduct quantitative information verification & validation of emerging cyber technologies. ***FY 2015 Plans:*** - Develop tools and techniques to rapidly configure cyber experiments. - Demonstrate cyber technologies with operationally relevant response time.			
Title: Embedded, Mobile & Tactical Environments (EMT) ***Description:*** Increase the overall emphasis on the Department's 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 smart phones, 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 Plans:*** - Develop monitoring and assessment tools to track behavior of embedded cyber systems. - Develop approaches to detect counterfeit components in embedded hardware. ***FY 2015 Plans:*** - Develop monitoring and assessment tools to track behavior of embedded cyber systems.	-	2.086	4.500
Accomplishments/Planned Programs Subtotals	10.542	13.907	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2015 Office of Secretary Of Defense			Date: March 2014
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)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• BA 3, PE #0603668D8Z, P113: *Cyber Advanced Technology Development*	11.103	9.667	-	-	-	-	-	-	-	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A