Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Office of Secretary Of Defense											DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*					R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*							
COST ($ in Millions)	**All Prior Years**	**FY 2012**	**FY 2013#**	**FY 2014 Base**	**FY 2014 OCO ##**	**FY 2014 Total**	**FY 2015**	**FY 2016**	**FY 2017**	**FY 2018**	**Cost To Complete**	**Total Cost**
Total Program Element	-	5.280	18.985	18.908	-	18.908	23.675	22.790	22.675	22.797	Continuing	Continuing
P003: *Cyber Applied Research*	-	5.280	18.985	18.908	-	18.908	23.675	22.790	22.675	22.797	Continuing	Continuing

FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

The FY 2014 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) networks to counter those threats and assure our missions. This 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.

The Cyber Applied Research program element is budgeted in the applied research budget activity because it emphasizes an approach to develop new security paradigms and architectures to enable agile cyber operations in a resilient and trustworthy cyberspace. These approaches will include 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 attack from an advanced, persistent cyber threat, and focusing on mission assurance. The Cyber Applied Research program builds on the existing basic and applied research results and transition new successful applied research results to the Cyber Advanced Technology Development program element (0603668D8Z).

This program focuses on integrating computer network defense and computer network operations, addressing the advanced persistent threat, and filling DoD technology gaps as identified in the 2012 Cyber Priority Steering Council Science & Technology Roadmap and assessments conducted by the Office of the Assistant Secretary of Defense for Research & Engineering (OASD(R&E)).

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Office of Secretary Of Defense	DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*

B. Program Change Summary ($ in Millions)	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total
Previous President's Budget	4.581	18.985	19.041	-	19.041
Current President's Budget	5.280	18.985	18.908	-	18.908
Total Adjustments	0.699	0.000	-0.133	-	-0.133
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	0.700	-			
• SBIR/STTR Transfer	-	-			
• Baseline Adjustments	-	-	-0.133	-	-0.133
• Other Adjustments	-0.001	-	-	-	-

Change Summary Explanation

Baseline adjustments are reflective of DoD priorities and requirements.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense			DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied Research*	

COST ($ in Millions)	All Prior Years	FY 2012	FY 2013#	FY 2014 Base	FY 2014 OCO ##	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
P003: *Cyber Applied Research*	-	5.280	18.985	18.908	-	18.908	23.675	22.790	22.675	22.797	Continuing	Continuing

FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

The FY 2014 OCO Request will be submitted at a later date

A. Mission Description and Budget Item Justification

The program is developing technology options through the DoD S&T organizations within and across the following technical areas:

INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
Develop technologies to harden DoD network components; evolve from network defense to mission assurance; and enable systems to operate through cyber attacks in degraded and contested environments.

COMPUTER NETWORK OPERATIONS (CNO):
Disrupt adversary attack planning and execution; explore game-changing ideas over the full spectrum of CNO and new concepts in cyber warfare; increase collaboration between disparate research communities within CNO; and address identified gaps in DoD CNO S&T to prepare for cyber conflict against advanced persistent threats.

CYBER METRICS AND EXPERIMENTATION:
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 scientific framework in which cyber security research can be conducted to test hypothesis with measurable and repeatable results, and quantitative experimentation and assessment of new cyber technologies.

Beginning in FY 2014, the program will expand 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. The six new technical thrust areas include:

TRUST:
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.

RESILIENT INFRASTRUCTURE:

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied Research*

Entails the ability to withstand cyber attacks, and sustain or recover critical functions. A resilient infrastructure has the ability to continue to perform its functions and provide its services to 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 covers ways to develop 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 resiliency architectures.

AGILE OPERATIONS:
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 relocation for altering the operating location 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.

ASSURING EFFECTIVE MISSIONS:
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. There is a critical need for tools that can map information technology assets to missions and use modeling and simulation, or other techniques, to perform dynamic analysis of asset criticality and course-of-action alternatives. 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.

CYBER MODELING, SIMULATION, AND EXPERIMENTATION (MSE):
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: Cyber Modeling and Simulation and 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 hypothesis with measurable and repeatable results, and the quantitative experimentation and assessment for new cyber technologies. These new methodologies will enable the exploration modeling and simulation tools and techniques that can drive innovation in research

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied 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.

EMBEDDED, MOBILE, AND TACTICAL ENVIRONMENTS (EMT):
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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2012	FY 2013	FY 2014
Title: Cyber Applied Research	5.280	18.985	18.908

Description: The Cyber Applied Research program builds on the existing basic and applied research results and transition new successful applied research results to the Cyber Advanced Technology Development program element. The link between the Cyber Applied Research and Cyber Advanced Technology Development program elements is intended to create a mechanism to take existing basic research results and mature them to the point of incorporation into technology demonstrations. This 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 & Technology Roadmap and assessments conducted by the Office of the Assistant Secretary of Defense for Research & Engineering (OASD(R&E)). Progress and results are reviewed by the DoD Cyber Science & Technology Priority Steering Council.

FY 2012 Accomplishments:
INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
- Established technique to detect and prevent attempts to re-flash BIOS or other firmware updates
- Established techniques to detect malicious Ethernet firmware/hardware (GOTS printed circuit board)
- Created Computer Network Defense (CND) framework to accelerate CND technology development through reuse of common services
- Developed initial design for user space anomaly detection and kernel protection for Linux systems
- Collaboration among NSA, CERDEC, and NRL improved through co-located work enabling development and Host Integrity analysis advancements

COMPUTER NETWORK OPERATIONS (CNO):
- Documented high assurance separation architecture using multi-core technology for application in tactical AIS environments

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2012	FY 2013	FY 2014
- Developed initial defense capabilities for the CNO framework - Complete time of flight measurement algorithm and initiated hybrid geo-location technique investigations CYBER METRICS AND EXPERIMENTATION: - Demonstrated a protection system that enhances mission assurance - Reported real-world reviews of reverse engineering framework -Demonstrated call graph monitoring as well as user-space runtime measurement ***FY 2013 Plans:*** FOUNDATIONS OF TRUST: - Develop scalable reverse engineering and analysis - Explore and identify trust establishment, propagation, and maintenance techniques - Enable measurement of trustworthiness - Develop trustworthy architectures and trust composition tools - Create cost-effective technology for the construction of high-assurance cyber-physical systems, meaning functionally correct and satisfying appropriate safety and security properties CYBER RESILIENCE: - Develop analytical model for routing techniques in the presence of jamming - Understand new mechanisms for secure operation of many-core chips - Develop methods for increasing resiliency of operational systems - Identify mechanisms to compose resilient systems from brittle components - Monitor, protect and reconfigure a host system or peripheral components that are targeted during an attack CYBER AGILITY: - Research and analyze the security architectures of various major web engines such as Trident and Gecko - Design distributed systems architectures and service application polymorphism ASSURING EFFECTIVE MISSIONS: - Research trusted information flow architectures, frameworks, and mechanisms for application to tactical AIS environments - Develop techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure - Develop techniques for course of action development and analysis - Improve Realism through automated mission modeling and mission situational awareness. ***FY 2014 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2012	FY 2013	FY 2014
FOUNDATIONS OF TRUST*: - Develop scalable reverse engineering and analysis - Explore and identify trust establishment, propagation, and maintenance techniques - Enable measurement of trustworthiness - Develop trustworthy architectures and trust composition tools - Detect malicious USB firmware/hardware using GOTS printed circuit board. CYBER RESILIENCE* - Develop methods for increasing resiliency of operational systems - Identify mechanisms to compose resilient systems from brittle components - Integrate sensing, detection, response, and recovery mechanisms - Design framework for secure modularization and virtualization of nodes and networks - Conduct resiliency-specific modeling and simulation - Develop code-level software resiliency - Develop advanced Computer Network Defense (CND) components and management features for the CND framework. CYBER AGILITY* - Design distributed systems architectures and service application polymorphism - Design network composition based on graph theory, distributed collaboration and social network theory - Develop techniques for autonomous reprogramming, reconfiguration, and control of cyber components, and machine intelligence - Develop automated reasoning techniques for executing courses of action ASSURING EFFECTIVE MISSIONS* - Develop techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure - Develop techniques for course of action development and analysis - Enable cyber effects assessment - Demonstrate Computer Network Operations (CNO) framework scalability in a representative laboratory environment (1000+ Nodes) CYBER MODELING, SIMULATION, AND EXPERIMENTATION (MSE)* - Derive experimentation metrics and techniques that apply to a suite of technologies - Determine accuracy of experimental results and applicability to operational environments - Demonstrate high fidelity network traffic emulation - Demonstrate cyber M&S integrated with traditional M&S			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Office of Secretary Of Defense		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602668D8Z: *Cyber Applied Research*	PROJECT P003: *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2012	FY 2013	FY 2014
- Develop M&S for large scale aggregate behavior EMBEDDED, MOBILE, AND TACTICAL ENVIRONMENTS (EMT)* - Develop monitoring and assessment tools to track behavior of embedded cyber systems - Develop approaches to detect counterfeit components in embedded hardware *FROM CYBER ROADMAP			
Accomplishments/Planned Programs Subtotals	5.280	18.985	18.908

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
• BA 3, PE #0603668D8Z, P113: *Cyber Advanced Technology Development*	5.836	19.935	19.668		19.668	29.221	30.337	30.831	31.431	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A