Exhibit R-2, **RDT&E Budget Item Justification:** PB 2013 Office of Secretary Of Defense	**DATE:** February 2012
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)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
Total Program Element	4.538	4.581	18.985	-	18.985	19.041	9.581	9.851	10.030	Continuing	Continuing
P003: *Cyber Applied Research*	4.538	4.581	18.985	-	18.985	19.041	9.581	9.851	10.030	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 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 Advanced Technology Development program element is budgeted in the advanced technology development budget activity because it will focus on the maturation of successful applied research results and their development into demonstrable advanced cyber capabilities. The Cyber Advanced Technology Development program will build on results of matured applied research from the Cyber Applied Research Program and other programs to develop technology demonstrations for potential transition into capabilities that support the full spectrum of computer network operations. 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.

This program focuses on integrating computer network defense and computer network operations, addressing the advanced persistent threat, and filling DoD technology gaps as determined by assessments conducted by the Office of the Assistant Secretary of Defense for Research & Engineering (OASD(R&E)) over the past year.

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2013 Office of Secretary Of Defense	**DATE:** February 2012
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 2011**	**FY 2012**	**FY 2013 Base**	**FY 2013 OCO**	**FY 2013 Total**
Previous President's Budget	10.000	9.735	19.519	-	19.519
Current President's Budget	4.538	4.581	18.985	-	18.985
Total Adjustments	-5.462	-5.154	-0.534	-	-0.534
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-0.300	-			
• SBIR/STTR Transfer	-0.117	-0.122			
• Congressional Adjustments	-5.000	-5.000	-	-	-
• Economic Assumptions	-0.025	-	-	-	-
• FFRDC	-0.018	-0.032	-	-	-
• Other Program Adjustments	-0.002	-	-0.534	-	-0.534

Exhibit R-2A, **RDT&E Project Justification:** PB 2013 Office of Secretary Of Defense		**DATE:** February 2012
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)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
P003: *Cyber Applied Research*	4.538	4.581	18.985	-	18.985	19.041	9.581	9.851	10.030	Continuing	Continuing

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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Title: Cyber Applied Research	4.538	4.581	18.985
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 determined by assessments in the Office of the Assistant Secretary of Defense for Research & Engineering. Progress and results are reviewed by the DoD Cyber S&T Steering Council. ***FY 2011 Accomplishments:*** Initiated research activities with the specific focuses technical areas of information assurance and computer network defense, computer network operations, and cyber metrics and experimentation. Commenced a semi-annual technical program review			

Exhibit R-2A, **RDT&E Project Justification:** PB 2013 Office of Secretary Of Defense		**DATE:** February 2012
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 2011**	**FY 2012**	**FY 2013**

cycle and a series of laboratory-hosted cross-fertilization workshops to enable joint collaboration across DoD S&T organizations and between the defensive and offensive S&T communities.

Focuses of each technical area:

INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
-Resilient architectures and protocols to reduce cyber reaction time for rapid system reconstitution to a known secure state and enable critical mission operation through cyber attacks in degraded environments.
-Agile cyber operations to enable moving target defense and defensive cyber maneuver.
-Attack detection and understanding to reduce, rapidly and autonomously detect, and mitigate attack effects.
-Vulnerability discovery and analysis to improve cyber risk assessment, situational awareness, and the impact of cyber assets on missions.

COMPUTER NETWORK OPERATIONS (CNO):
-Resilient CNO frameworks and architectures.
-Wireless discovery and access techniques.
-Situational awareness in near real-time during cyber operations.
-Agile cyber maneuver to disrupt and confuse adversarial attack planning cycles to increase adversary risk and work factor and decrease effectiveness during adversary attack and exploitation attempts.
-Improved understanding of the adversarial threat.

CYBER METRICS AND EXPERIMENTATION:
-Measurements of effectiveness of existing countermeasures and the current level of DoD cyber security.
-Measurements of impacts of new cyber security technologies.
-Measurements of computer and network assurance levels for enhanced situational awareness.
-Quantitative analysis and experimental testing of the effect of resilient and agile cyber operations and architectures on DoD system and network security.

FY 2012 Plans:
INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
-Enable interoperability amongst computer network defense and computer network attack software framework capabilities for broader threat mitigation coverage.
-Develop analytical model of resiliency of cross-layer protocols and routing techniques in the presence of jamming.
-Investigate vulnerabilities in rich content delivery in new implementations of common web browsers.

Exhibit R-2A, **RDT&E Project Justification:** PB 2013 Office of Secretary Of Defense		**DATE:** February 2012
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 2011**	**FY 2012**	**FY 2013**

-Test and evaluate existing type-checking, shadow circuits, and other security mechanisms in use by separation kernels.
-Investigate optical transport layer vulnerabilities in commoditized critical infrastructure systems, including fiber-optic telecommunications devices.
-Develop non-signature-based monitoring and validation methods to accurately convey the integrity of running system software.

COMPUTER NETWORK OPERATIONS (CNO):
-Development of common protocols and services to enable a common command and control infrastructure and more efficient effects development to enhance existing but disparate computer network operations software frameworks.
-Develop and test a time difference of arrival system for tactical wireless emitter localization.
-Design and develop algorithms and techniques for data hiding at the physical layer of wireless networks.
-Examine the scale and breadth of control that provides adversaries a broad base from which to launch cyber attacks using botnets.

CYBER METRICS AND EXPERIMENTATION:
-Development of a composite trust metric and mission performance tradeoff analysis for mobile ad-hoc networks (MANETs).

FY 2013 Plans:
INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
-Investigate impact of cognitive radio technology to increase network resiliency by enabling cross-layer communications.
-Define hardware/software interface logic language for many-core processors and systems on a chip to integrate security into automated design flows and run time systems.
-Develop improved security framework for optical transport layers in critical infrastructure fiber-optic telecommunications devices to ensure reliability and availability of critical communications networks to both DoD and commercial operators and users.
-Develop techniques to employ non-signature-based monitoring and validation methods to make trust decisions on information systems.

COMPUTER NETWORK OPERATIONS (CNO):
-Decouple programming language-dependent constructs in existing CNO software frameworks to allow for development of clients developed in different languages to operate within the SW architecture.
-Investigate and test a hybrid time of arrival and phased array system for wireless localization.
-Construct wireless environments for implementing authentication and information hiding schemes at the physical later of wireless networks.
-Demonstrate malicious code delivery through audio and video content vulnerabilities new implementations of common web browsers.

Exhibit R-2A, **RDT&E Project Justification:** PB 2013 Office of Secretary Of Defense		**DATE:** February 2012
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 2011	FY 2012	FY 2013
-Develop techniques to address adversarial botnets in real-time. CYBER METRICS AND EXPERIMENTATION: -Optimization of a composite trust metric and application for risk management and mission performance tradeoff analysis for multiple-objective missions in coalition networks.			
Accomplishments/Planned Programs Subtotals	4.538	4.581	18.985

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
• BA 3, PE #0603668D8Z, P113: *Cyber Advanced Technology Development*	4.847	5.539	19.935		19.935	19.995	29.707	30.783	31.342	Continuing	Continuing

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A