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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*

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	-	5.836	19.935	19.668	-	19.668	29.221	30.337	30.831	31.431	Continuing	Continuing
P113: *Cyber Advanced Technology Development*	-	5.836	19.935	19.668	-	19.668	29.221	30.337	30.831	31.431	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 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 through exploring and exploiting 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 focuses on the maturation of successful applied research results, and their development, into demonstrable advanced cyber security capabilities. The Cyber Advanced Technology Development program will build on the results of matured applied research from the Cyber Applied Research (0602668D8Z), 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 an attack from an advanced persistent cyber threat, and focusing on mission assurance metrics.

This program focuses on integrating computer network defense (CND) and computer network operations (CNO), in addressing the advanced persistent threat (APT), filling DoD technology gaps as identified in the FY 2012 Cyber Priority Steering Council Science & Technology Roadmap, as determined by 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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*

B. Program Change Summary ($ in Millions)	**FY 2012**	**FY 2013**	**FY 2014 Base**	**FY 2014 OCO**	**FY 2014 Total**
Previous President's Budget	5.539	19.935	19.995	-	19.995
Current President's Budget	5.836	19.935	19.668	-	19.668
Total Adjustments	0.297	0.000	-0.327	-	-0.327
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	0.299	-			
• SBIR/STTR Transfer	-	-			
• Baseline Adjustments	-	-	-0.327	-	-0.327
• Other Adjustments	-0.002	-	-	-	-

Change Summary Explanation

FY 2014 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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*	**PROJECT** P113: *Cyber Advanced Technology Development*

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
P113: *Cyber Advanced Technology Development*	-	5.836	19.935	19.668	-	19.668	29.221	30.337	30.831	31.431	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

Efforts of the program will develop improved and demonstrable capabilities through the DoD science and technology (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.

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:

FOUNDATIONS OF 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:
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 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

cover 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 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):

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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*	**PROJECT** P113: *Cyber Advanced Technology Development*

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 Advanced Technology Development	5.836	19.935	19.668

Description: The Cyber Advanced Technology Development program will build on, mature, and transition 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 program elements (PEs) 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 Cyber S&T Priority Steering Council.

FY 2012 Accomplishments:
INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (IA/CND):
- Developed a composite trust metric for MANETs and coalition networks
- Developed trust-based multi-objective optimizations for coalition networks
- Integrated expanded startup measurements of Windows, Linux and virtualized platforms
- Created Computer Network Defense (CND) framework to accelerate CND technology development through reuse of common services
- Demonstrated operational pilots of host integrity, including as startup (NSA EHI-EM) and adding runtime
- Developed command authentication patch to prevent hijacking of untrusted optical transport equipment
- Demonstrated techniques to identify all publically known zero-day exploits in FY 2012

COMPUTER NETWORK OPERATIONS (CNO):
- Created data communication standard to support interoperability among service implemented Computer Network Operations (CNO) software frameworks
- Demonstrated unidirectional variable format messages (VMF) data transfer from low to high for a tactical cross domain solution (CDS) for the individual dismounted soldier

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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*	**PROJECT** P113: *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2012**	**FY 2013**	**FY 2014**

CYBER METRICS AND EXPERIMENTATION:
- Developed and tested relevant technologies to improve the functionality of Cyber Ranges

FY 2013 Plans:

FOUNDATIONS OF TRUST:
- Report on the design and analysis of the composite trust model
- Report comparing the proposed trust framework on network security to existing mechanisms with similar purposes
- Develop framework for collaborative reverse engineering
- Conduct real world red team testing reviews using the Chimera framework
- Demonstrate the application of trusted computing and measurement technologies to a modern cloud computing infrastructure

CYBER RESILIENCE:
- Document high assurance separation architecture using multi-core technology for applications in tactical AIS environments
- Improve CND decision making through data sharing by enabling disparate CND technologies
- Develop Common Protocols and Open API's
- Demonstrate fully operational protection system that enhances mission assurance
- Augment an evolving set of mission assurance services to specifically counter APT effects at the operational level

CYBER AGILITY:
- Demonstrate fingerprinting capabilities and identify vulnerabilities in HTML5 for rich content
- Develop countermeasures to mitigate hardware and firmware based attacks
- Demonstrate fully operational protection system that enhances mission assurance
- Characterize the APT against the agility/maneuver defensive technologies, enabling direct assessment of effectiveness against an APT-class threat

ASSURING EFFECTIVE MISSIONS:
- Develop trust management schemes to capture mission performance metrics in tactical networks
- Develop means for identifying and monitoring of steganography while assuring integrity of data channels

CYBER MODELING, SIMULATION, AND EXPERIMENTATION:
- Practical input/output metrics for assessment of classified technologies associated with offensive, defensive, and mission oriented capabilities
- Provide opportunities for cross-service and cross-CTS multi-disciplinary experiments using the Joint I/O range

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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*	**PROJECT** P113: *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2012**	**FY 2013**	**FY 2014**
- Demonstrate the use of Graphical Processor Units (GPUs) and multicore processors to dramatically increase the computational parallelism available to model and simulate cyberspace effects on a country or global scale. EMBEDDED, MOBILE, AND TACTICAL ENVIRONMENTS: - New hybrid time of arrival / phased array antenna system for protocol-independent ability to geo-locate wireless emitters - Develop analytical model of the resiliency of routing techniques in the presence of wireless jamming ***FY 2014 Plans:*** FOUNDATIONS OF TRUST*: - Develop scalable reverse engineering and analysis - Explore and identify trust establishment, propagation, and maintenance techniques - Develop trustworthy architectures and trust composition tools - Integrate userspace integrity measurements with larger system measurement 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 - Pilot host integrity for virtual platforms 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 - Integrate advanced Computer Network Defense (CND) components and management features into the CND framework 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*:			

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 3: *Advanced Technology Development (ATD)*	**R-1 ITEM NOMENCLATURE** PE 0603668D8Z: *Cyber Advanced Technology Development*	**PROJECT** P113: *Cyber Advanced Technology Development*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2012**	**FY 2013**	**FY 2014**
-Develop approaches and tools to incorporate models of the cyber substrate in kinetic simulations -Develop cyber and simulation models that incorporate mission models and cyber-kinetic effects -Establish game and a decision-theoretic and other approaches to infer and predict adversary intentions, strategies, and tactics - Develop large-scale experiments to explore a variety of adversarial behaviors and defensive postures EMBEDDED, MOBILE, AND TACTICAL ENVIRONMENTS: -Establish architectural approaches for composing embedded mobile systems (smart phones, tablets, and mobile applications) within an overarching system and develop the security capabilities needed to make the composed system robust and secure -Identify mechanisms for trust establishment and secure information sharing at the tactical edge -Develop approaches to security and mobility-aware routing and quality of service *FROM CYBER ROADMAP			
Accomplishments/Planned Programs Subtotals	5.836	19.935	19.668

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 2, PE # 0602668D8Z, P003: *Cyber Applied Research*	5.280	18.985	18.908		18.908	23.675	22.790	22.675	22.797	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A