Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Defense Advanced Research Projects Agency										DATE: February 2012	
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*				R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*							
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	239.631	354.125	392.421	-	392.421	428.541	455.164	457.831	493.760	Continuing	Continuing
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	74.976	85.358	107.371	-	107.371	115.168	115.092	116.092	121.704	Continuing	Continuing
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	109.608	178.419	170.642	-	170.642	174.185	185.491	190.491	195.808	Continuing	Continuing
IT-04: *LANGUAGE TRANSLATION*	55.047	67.015	64.408	-	64.408	72.521	71.248	51.248	51.248	Continuing	Continuing
IT-05: *CYBER TECHNOLOGY*	-	23.333	50.000	-	50.000	66.667	83.333	100.000	125.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information and Communications Technology program element is budgeted in the applied research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies.

The High Productivity, High-Performance Responsive Architectures project is developing the necessary computing hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include supercomputer, embedded computing systems, and novel design tools for manufacturing of defense systems.

The Information Assurance and Survivability project is developing the technology required to make emerging information system capabilities (such as wireless and mobile code/mobile systems) inherently secure, and to protect DoD's mission-critical systems against attack upon or through the supporting information infrastructure. These technologies will enable our critical systems to provide continuous correct operation even when they are attacked, and will lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites.

The Language Translation project will develop and test powerful new Human Language Technology that will provide critical capabilities for a wide range of national security needs. This technology will enable systems to a) automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means; b) to have two-way (foreign-language-to-English and English-to-foreign-language) translation; c) enable automated transcription and translation of foreign speech and text along with content summarization; and d) enable exploitation of captured, foreign language hard-copy documents.

The Cyber Technology project supports long term national security requirements through the development and demonstration of technology to increase the security of military information systems. This involves networking, people, platforms, weapons sensors, and decision aids to create a whole that is greater than the sum of

its parts. The results are networked forces that operate with increased speed and synchronization and are capable of achieving massed effects without the physical massing of forces as required in the past.

B. Program Change Summary ($ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Previous President's Budget	281.262	400.499	368.621	-	368.621
Current President's Budget	239.631	354.125	392.421	-	392.421
Total Adjustments	-41.631	-46.374	23.800	-	23.800
• Congressional General Reductions	-1.287	-			
• Congressional Directed Reductions	-28.000	-46.374			
• Congressional Rescissions	-5.837	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	0.011	-			
• SBIR/STTR Transfer	-6.518	-			
• TotalOtherAdjustments	-	-	23.800	-	23.800

Change Summary Explanation

FY 2011: Decrease reflects reductions for the Section 8117 Economic Adjustment, contract award delays, rescissions, and the SBIR/STTR transfer offset by internal below threshold reprogrammings.

FY 2012: Decrease reflects reductions for unsustained funding and reduction to new starts.

FY 2013: Increase reflects increased emphasis on fab-less design manufacturing, more efficient high performance computing and cyber security.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency			DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	

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
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	74.976	85.358	107.371	-	107.371	115.168	115.092	116.092	121.704	Continuing	Continuing

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computer hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems. One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build large complex software systems. Powerful new approaches and tools are needed to enable the rapid and efficient production of new software, including software that can be easily changed to address new requirements and can adjust dynamically to platform and environmental perturbations. The project will ensure accessibility and usability to a wide range of application developers, not just computational science experts. This project will also focus on novel design tools for the manufacture of complex ground and aerospace systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Title: META	49.000	56.000	75.000

Description: The goal of the META program is to develop novel design flows, tools, and processes to enable a significant improvement in the ability to design complex defense and aerospace systems that are correct-by-construction. The program seeks to develop a design representation of meta-language and a domain-specific component model library from which system designs can quickly be assembled and their correctness verified with a high degree of certainty. Such a "fab-less" design approach is complemented by a foundry-style manufacturing capability, consisting of a factory capable of rapid reconfiguration between a large number of products and product variants through bitstream reprogramability, with minimal or no resultant learning curve effects. Together, the fab-less design and foundry-style manufacturing capability is anticipated to yield substantial---by a factor of five to ten---compression in the time to develop and field complex defense and aerospace systems.

The META effort will also explore the initial design of a next generation ground vehicle by employing a novel, model-based correct-by-construction design capability, a highly-adaptable foundry-style manufacturing capability, and crowd-sourcing methods to demonstrate 5x-10x compression in the timeline necessary to build an infantry fighting vehicle. Beginning in FY 2012, the specific ground vehicle application work will be funded in PE 0602702E, Project TT-04, Advanced Land Systems.

FY 2011 Accomplishments:

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Continued development and integration of supporting tools necessary to implement the model-based design, integration, and verification flows. - Continued development of a foundry configuration toolset to enable the (re)configuration of foundry-style manufacturing capabilities for a given required degree of manufacturing adaptability. - Exercised feedback loop between manufacturability constraints and the system design toolset. - Continued development and testing of crowd-sourced design infrastructure for electromechanical and software systems for a next generation ground combat vehicle. ***FY 2012 Plans:*** - Mature the initial set of tools developed to implement model-based design, integration and verification to a productized version that may be released for open use with an appropriate license and will be utilized by the crowd-sourced design infrastructure. - Develop a domain-specific component model library for the drivetrain/mobility subsystems and the chassis/survivability systems of a military ground vehicle through extensive characterization of desirable and spurious interactions, dynamics, and properties of all constituent components down to the numbered part level. - Develop context models to reflect various operational environments. - Develop a domain-specific foundry configuration for military ground vehicles. - Begin the assembly and integration of foundry-style manufacturing capability for military ground vehicles. - Develop and implement an infrastructure for publishing and maintaining detailed component models using the metalanguage construct to expand the design space for subsequent efforts to design and build a military ground vehicle. - Develop a mechanism for the feedback of manufacturability constraints into the design and design tradespace exploration process. - Develop and integrate a library of various fabrication processes and associated manufacturing elements, i.e., machines and techniques employed to produce the various constituent elements of the military ground vehicle. ***FY 2013 Plans:*** - Develop a domain-specific component model library for an entire military ground vehicle through extensive characterization of desirable and spurious interactions, dynamics, and properties of all constituent components down to the numbered part level. - Finalize development of the foundry-style manufacturing capability for military ground vehicles. - Utilize the iFAB foundry to fabricate the drivetrain and mobility subsystem winning design from the related challenge. - Utilize the iFAB foundry to fabricate the chassis and survivability subsystem winning design from the related challenge.			
Title: Power Efficiency Revolution For Embedded Computing Technologies (PERFECT)* ***Description:*** * Includes aggregation of the Ubiquitous High Performance Computing (UHPC) and Architecture Aware Compiler Environment (AACE) programs.	22.270	24.126	25.371

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
The Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) program will provide the technologies and techniques to overcome the power efficiency barriers which currently constrain embedded computing systems capabilities and limit the potential of future embedded systems. The warfighting problem this program will solve is the inability to process future real time data streams. This is a challenge for embedded applications, from Intelligence, Surveillance and Reconnaissance (ISR) systems on unmanned air vehicles through combat and control systems on submarines. The PERFECT program will overcome processing power efficiency limitations using threshold voltage operation, massive and heterogeneous processing concurrency, new architecture concepts, hardware and software approaches to address system resiliency, combined with software approaches to effectively utilize resulting system concurrency to provide the required embedded system processing power efficiency. ***FY 2011 Accomplishments:*** - Identified, researched, and initiated the evaluation of critical technologies, system methodologies, and architectures supporting UHPC program goals. - Completed the description of two UHPC challenge problems, synthetic aperture radar processing and graph-analysis. - Released static system characterization tools to enhance compiler performance. - Developed automatic idiom recognition tool (identify patterns of computation and data access) to support algorithm analysis, development, and implementation. ***FY 2012 Plans:*** - Complete UHPC high level architectural designs. - Release runtime system support tools for attributing runtime costs and pinpointing system performance and stability bottlenecks. - Develop interactive compilation framework incorporating affine (linear loop parallelization) and software pipelining (find and exploit parallelization in serial codes) optimizations to automate code parallelization. - Release dynamic system and performance characterization tools to enhance compiler performance via runtime performance feedback, incorporating the use of off line learning engines. ***FY 2013 Plans:*** - Discover power kernels for embedded DoD applications, including intelligence, surveillance and reconnaissance (ISR) and encryption capabilities. - Establish initial simulation infrastructure for evaluating temporal and power efficiency for DoD embedded subsystems. - Develop theoretical near threshold voltage and resiliency trade-offs for power efficiency, to be followed by experimental validation. - Identify key language extensions and approaches required for the development of massively parallel software.			
Title: Military Critical Clouds (MCC)	-	-	7.000

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	**R-1 ITEM NOMENCLATURE** PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**PROJECT** IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Description: The Military Critical Clouds (MCC) program will bring the advantages of the cloud computing paradigm to mission-critical military applications and combat systems. The advantages of cloud computing have been demonstrated in civilian and Government applications to include the efficient utilization of computing resources, enabling deployed systems to be upgraded in the field, and reduced recurring and non-recurring costs. With cloud computing, myriad one-of-a-kind, single platform specific processing implementations are eliminated and replaced with application effective computing on common hardware. To date, the cloud computing paradigm has not been effectively exploited in embedded military applications, for reasons related to performance and correctness constraints. In order to apply the cloud paradigm to military systems, MCC will make significant advances in the areas of virtualization, real-time responsiveness, reliability and verifiability, and security, while taking advantage of the cloud computing paradigm's inherent cost efficiency, manufacturing agility, maintainability, and programming democratization. Fully realizing these capabilities will open the door to "platform clouds" that provide dramatically improved effectiveness in our military combat systems. ***FY 2013 Plans:*** - Develop an overarching architecture and operational concept that applies the cloud computing paradigm to selected mission-critical military applications and combat systems. This will include the interactions of real-time requirements, quality of service guarantees, dynamic adaptivity, and system-level performance verification. - Create a modeling and simulation capability and quantify the potential improvement of cloud-based combat systems vice conventional approaches. - Define challenge problems, based on existing and near-term future DoD embedded systems. These problems will be used to focus research and assess progress.			
Title: High-Productivity Computing Systems (HPCS) ***Description:*** The High-Productivity Computing Systems (HPCS) program is creating a new generation of economically viable, high-productivity computing systems for the national security and industrial user communities. HPCS technologies will enable nuclear stockpile stewardship, weapons design, cryptanalysis, weather prediction, and other large-scale problems that cannot be addressed productively with today's computers. The goal of this program is to develop revolutionary, flexible and well-balanced computer architectures that will deliver high performance with significantly improved productivity for a broad spectrum of applications. Additionally, programming such large systems will be made easier so engineers and scientists can better harness the power of high-performance computers. ***FY 2011 Accomplishments:*** - Fabricated and tested the final version of a terabits-per-second hub chip that will enable the first petascale system with global shared memory.	3.706	5.232	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Constructed, tested and started software integration of the first compute blades containing final version of all hardware components. ***FY 2012 Plans:*** - Monitor the two HPCS performers until program completion and complete prototype demonstrations with stakeholders.			
Accomplishments/Planned Programs Subtotals	74.976	85.358	107.371

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency			DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	

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
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	109.608	178.419	170.642	-	170.642	174.185	185.491	190.491	195.808	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information Assurance and Survivability project is developing the core computing and networking technologies required to protect DoD's information, information infrastructure, and mission-critical information systems. These technologies will enable DoD information systems to operate correctly and continuously even when they are attacked, and will provide cost-effective security and survivability solutions. Technologies developed under this project will benefit other projects within this program element as well as projects in the Command, Control, and Communications program element (PE 0603760E), the Network-Centric Warfare Technology program element (PE 0603764E), the Sensor Technology program element (PE 0603767E), and other projects that require secure, survivable, network-centric information systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Title: Cyber Genome	13.000	24.000	20.160

Description: The Cyber Genome program develops techniques to automatically characterize, analyze, and identify malicious code and determine the evolutionary relationship between new never-before-seen malware samples and older known malware. This enables the automatic detection and extermination of future malware variants. Such automation is critically important because the global production of malware is growing explosively and threatens to overwhelm current labor-intensive practices. Cyber Genome also develops advanced capabilities to enable positive identification of malicious code substructures and functionality.

FY 2011 Accomplishments:
- Expanded and refined technologies, ontologies, and algorithms to enable the characterization of future malicious code variants based on analyzed malicious code substructures.
- Completed integration of automatic discovery, identification, analysis, and prediction algorithms.
- Completed initial experiments on a large commercial mass-infection malware data set.

FY 2012 Plans:
- Create lineage trees for a class of digital artifacts for better software evolution forensics.
- Generate execution trees from submitted malware that include automated analysis of software dependencies.
- Implement techniques in a prototype system, demonstrate, and commence transition.

FY 2013 Plans:
- Extend and refine lineage trees for a class of digital artifacts.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Extend execution trees from submitted malware that include automated analysis of software dependencies. - Develop operationally relevant use-case test scenarios with transition partner and conduct initial use case validation tests.			
Title: Integrity Reliability Integrated CircuitS (IRIS)	22.878	30.000	20.000

Description: The U.S. military now consumes only approximately one percent of the total integrated circuit (IC) production in the world and increasingly relies on foreign foundry and supplier sources for ICs used within its systems. Given the relatively low consumption, the U.S. military IC requirements are not a factor that can influence IC production or the assurance that parts are delivered as specified. With the majority of ICs used in modern military systems fabricated offshore, this situation presents a potential future risk that the parts acquired will not operate only in the specified manner. The objective of the Integrity and Reliability of Integrated CircuitS (IRIS) program is to develop the technology to derive the functionality of an IC to determine unambiguously if malicious modifications have been made to that IC, and to accurately determine the IC's useful lifespan from a physical perspective. The IRIS program will develop nondestructive scientifically based techniques for full functionality identification and functionality modification detection for ICs utilized in military systems. In addition, the IRIS program will develop innovative test technologies and processes that can determine an IC's useful lifespan based on a significantly reduced number of samples. Once developed, the resulting technologies may be deployed to Government or appropriate organizations that can provide critical IC functionality and reliability inspection services to the DoD, thereby ensuring that a scientific means is available to determine functionality and reliability in the various ICs deployed in DoD systems.

FY 2011 Accomplishments:
- Completed designs of digital IC test articles for functional derivation.
- Completed designs of mixed-signal IC test articles for functional derivation.
- Completed designs of digital and mixed-signal IC test articles for reliability studies.

FY 2012 Plans:
- Complete fabrication of digital and mixed-signal IC test articles for functional derivation and reliability studies.
- Complete definition of functional requirements for algorithms that determine circuit functionality without prior knowledge of their underlying logic and design.
- Demonstrate functional derivation of un-altered digital and mixed-signal ICs at the 45 nm complementary metal-oxide semiconductor (CMOS) node.
- Demonstrate reliability derivation from reduced sample sizes of digital ICs at the 90 nm node and mixed-signal ICs at the 130 nm node.
- Develop tools for functional derivation from third-party Intellectual Property (IP) blocks for both Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs).

FY 2013 Plans:

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Demonstrate functional derivation of modified digital and mixed-signal ICs at the 45 nm CMOS node. - Demonstrate reliability derivation from reduced sample sizes of modified ICs. - Demonstrate non-destructive techniques for reverse engineering a digital IC. - Demonstrate tools for functional derivation from third-party IP (Intellectual Property) blocks for both ASICs and FPGAs.			
Title: Cyber Fast Track* ***Description:*** *Formerly Agile Assured Computing The Cyber Fast Track program will create more flexible, responsive methods for securing computing systems that operate in challenging environments and will reduce security risk without requiring lengthy development cycles. Under Cyber Fast Track, small agile teams will work under rapid development cycles to create cyber-security applications responsive to pop-up threats identified by DoD. This is in contrast to the current commercial security paradigm of large, highly complex, security systems that add layer upon layer of functionality and that, in themselves, are difficult to maintain and are vulnerable to attack. ***FY 2011 Accomplishments:*** - Identified mechanisms to determine outdated and unnecessary system attributes used for attacks and approaches for modifying those attributes to provide a secure operating pathway. - Initiated development of techniques for mobile endpoint security and live environment testing. - Initiated development of techniques for measurement of dynamic code, detection of vulnerabilities and exploitable bugs, and cyber automation and control. ***FY 2012 Plans:*** - Refine and update pop-up threat list with CYBERCOM. - Develop tools, methods, and techniques to reduce attack surface areas. - Demonstrate tools, methods, and techniques to reduce attack surface areas. ***FY 2013 Plans:*** - Further refine and update pop-up threat list with CYBERCOM. - Broaden tools, methods, and techniques to reduce attack surface areas. - Further demonstrate tools, methods, and techniques to reduce attack surface areas. - Transition the Cyber Fast Track business model to other DoD agencies.	5.349	10.000	17.800
Title: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) ***Description:*** The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program will develop cyber security technologies using the mechanisms of biological systems as inspiration for radically re-thinking basic hardware and system	15.000	29.000	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013

designs. Higher level organisms have two distinct immune systems: the innate system is fast and deadly but is only effective against a fixed set of pathogens; the adaptive system is slower, but can learn to recognize novel pathogens. Similarly, CRASH will develop mechanisms at the hardware and operating system level that eliminate known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH will also develop software techniques that allow a computer system to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH will develop techniques that make each computer system appear unique to the attacker and allow each system to change over time.

FY 2011 Accomplishments:

- Developed initial system designs and implemented prototypes of two novel tagged security processors.
- Demonstrated through formal methods, simulation, and design walkthroughs that the prototype processors mitigate the top technical vulnerabilities.
- Implemented and validated rootkit detection capability in router operating system.
- Identified vulnerability in widely used embedded devices and developed mitigation and prevention techniques.
- Demonstrated low cost automatic patch generation for vulnerable systems.
- Demonstrated capabilities to roll-back a faulty system, install a patch, and then restore current state as if fault had never been present.
- Demonstrated initial policy weaver system that rewrites a given program into one that is guaranteed to enforce a stated security policy.
- Implemented formal verification system for operating system verification that achieves scalability by merging multiple domain specific logics, each corresponding to an abstraction layer of the operating system.
- Demonstrated a novel compiler that generates distinct variant binary files for every new compilation of the source code.

FY 2012 Plans:

- Implement two complete CRASH hardware tagged security processors capable of defeating common vulnerabilities and supporting novel, provably secure prototype operating systems.
- Demonstrate full scale systems capable of detecting and recovering from penetrations.
- Verify that known technical vulnerabilities have been addressed successfully using red team methods.
- Scale automatic patch generation to more complete coverage and to work on commercial scale systems.
- Automatically synthesize, using formal methods, hundreds of variants of a single distributed protocol, each of which is automatically proven correct.
- Implement a compiler that generates thousands of unique variants of programs that are demonstrated to be robust against return oriented programming attacks.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Demonstrate web-application environment that employs information flow to produce applications with strong information confidentiality guarantees without requiring additional effort by the application developer in order to maintain the guarantees. - Transition CRASH research into one or more commercial software applications. ***FY 2013 Plans:*** - Demonstrate moving target defense with automatically constructed diverse implementations of algorithms and programs. - Implement web-based application on secure operating system and verify its resistance to attacks through heterogeneity. - Produce formally-verified operating system kernel. - Integrate CRASH tagged security processor prototypes with secure operating system, development environments for correct-by-design software, and multiple applications. - Verify system integrity with focused red-team validation. - Demonstrate roll-back and recovery on production-scale system with substantially reduced human involvement. - Demonstrate, using policy weaving, automated implementation of security policies in applications and operating systems for a broad range of security policy frameworks. - Transition CRASH research products onto commercial router for military use.			
Title: Safer Warfighter Computing (SAFER)	13.275	20.000	24.180
Description: The Safer Warfighter Computing (SAFER) program is creating a technology base for assured and trustworthy Internet communications and computation, particularly in untrustworthy and adversarial environments. SAFER creates automated processes and technologies enabling military users to send and receive content on the Internet, utilizing commercially available hardware and software, in ways that avoid efforts to deny, locate, or corrupt communications. SAFER is also developing technology for performing computations on encrypted data without decrypting it first through fully homomorphic encryption and interactive, secure multi-party computation schemes. This will enable, for example, the capability to encrypt queries and to create an encrypted search result without decrypting the query. This technology will advance the ability to run programs on untrusted hardware while keeping programs, data, and results encrypted and confidential. This mitigates the important aspect of supply chain compromise. ***FY 2011 Accomplishments:*** - Developed technical approaches for improving the security of internet-based communications and computation supporting instant messaging and web search. - Demonstrated initial security, availability, encryption, and measurement capabilities. - Developed initial homomorphic encryption implementation and new data structures to support optimized implementations of fully homomorphic encryption.			

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Began second generation fully homomorphic encryption algorithm development. ***FY 2012 Plans:*** - Demonstrate enhanced security and availability capabilities with order of magnitude increase in scalability and support for full web surfing in addition to existing applications. - Perform initial independent, adversarial assessment of effectiveness of SAFER technologies to prevent communication localization and detection. - Continue development of decoy routing to support unblockable connectivity short of complete disconnection from the Internet. - Implement rich policy support for onion routing to enhance anonymity in the face of compromised routers. - Perform initial, independent benchmarks of fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation. - Design program-wide application programming interfaces (APIs) for low level mathematics and cryptography to support encrypted computation using either fully homomorphic encryption or secure multiparty computation. - Demonstrate optimized software implementations of second generation fully homomorphic encryption algorithms. ***FY 2013 Plans:*** - Perform follow up independent, adversarial assessment of effectiveness of SAFER technologies to prevent communication localization and detection, including newly developed adversarial techniques. - Demonstrate field programmable gate array implementation of fully homomorphic encryption offering order of magnitude in performance improvement over optimized software implementation. - Perform follow up, independent benchmarks of fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation. - Design program-wide APIs for cryptographic protocols to support encrypted computation using either fully homomorphic encryption or secure multiparty computation. - Implement prototype for new programming language to support computation on encrypted data.			
Title: Anomaly Detection at Multiple Scales (ADAMS) ***Description:*** The Anomaly Detection at Multiple Scales (ADAMS) program will develop and apply algorithms for detecting anomalous, threat-related behavior of systems, individuals, groups/organizations, and nation-states over hours, days, months, and years. ADAMS will develop flexible, scalable and highly interactive approaches to extracting actionable information from information system log files, sensors, and other instrumentation. ***FY 2011 Accomplishments:*** - Conceptualized approaches for finding indicators of anomalous behaviors buried in petabytes of observational data. ***FY 2012 Plans:***	4.500	18.000	12.502

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Prototype a scalable, distributed architecture to correlate relevant data from heterogeneous sources over extended periods of time. - Formulate techniques for determining whether a system, individual, group/organization, or nation-state is exhibiting anomalous behavior suggestive of a threat. - Develop technologies specific to the problem of detecting malicious insiders. ***FY 2013 Plans:*** - Demonstrate the capability to identify anomalous behavior suggestive of a threat. - Quantify probabilities of detection and false alarm for anomalous behaviors from measured threat profiles. - Characterize techniques for detecting malicious insiders.			
Title: Resilient Clouds* ***Description:*** *Formerly Resilient Networks The Resilient Clouds program will create technologies to enable cloud computing systems to survive and operate through cyber attacks. Vulnerabilities found in current standalone and networked systems will be amplified in cloud computing environments. Resilient Clouds will address this by creating advanced network protocols and new approaches to computing in potentially compromised distributed environments. Particular attention will be focused on adapting defenses and allocating resources dynamically in response to attacks and compromises. Resilient Clouds will create new approaches to measuring trust, reaching consensus in compromised environments, and allocating resources in response to current threats and computational requirements. Resilient Clouds will develop new verification and control techniques for networks embedded in clouds that must function reliably in complex adversarial environments. ***FY 2012 Plans:*** - Identify algorithmic advances and protocol re-design opportunities and requirements to achieve high levels of assurance in networked/cloud computing systems. - Design new algorithms and protocols in high-assurance implementations for use in networked/cloud computing systems. - Develop techniques for presenting a diverse, changing target to attackers without impacting the usability of applications running on these systems. - Create approaches and algorithms for expanding self-monitoring hosts into a cooperative self-monitoring cloud. ***FY 2013 Plans:*** - Measure the effectiveness of new algorithms and protocols for high-assurance computing in cloud computing systems that are under attack.	-	20.000	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Demonstrate a cloud computing environment that produces correct, mission-relevant results when individual computing elements have been compromised. - Validate the extension of host-level monitoring and adaptation to cloud-level monitoring and adaptation.			
Title: High Assurance Cyber Military Systems*	-	8.250	17.000
Description: *Formerly Assured Mobile Platform The High Assurance Cyber Military Systems program will develop and demonstrate the technologies required to secure mission-critical embedded computing systems. The DoD is making increasing use of networked computing in systems such as military vehicles, weapon systems, ground sensors, smartphones, personal digital assistants, and other communication devices. This dependence makes it critically important that the embedded operating system provides high levels of inherent assurance. This operating system must also integrate the computational, physical, and networking elements of the system while running on a processor with very limited size, weight, and power. Consequently, it can only devote a limited share of its computational resources to security while satisfying hard real-time constraints. Recent advances in program synthesis, formal verification techniques, low-level and domain-specific programming languages, and operating systems mean that fully verified operating systems for embedded devices may be within reach at reasonable costs. Systems that admit static verification can provide both high assurance and high performance to avoid the many dynamic checks otherwise necessary to provide high assurance. The program will develop, mature, and integrate these technologies to produce an embedded computing platform that provides a high level of assurance for mission-critical military applications. ***FY 2012 Plans:*** - Perform detailed requirements and systems engineering analyses to identify embedded devices requiring high assurance levels and a corresponding concept of operations. - Produce a high-level design for identified embedded computing platforms that provides a high level of assurance for military users. - Develop approaches to reduce the time to produce high-assurance embedded systems by leveraging existing high assurance systems, either through a modular architecture or through tool reuse. ***FY 2013 Plans:*** - Build tools to assist in the rapid creation of high-assurance embedded computing systems on a variety of architectures. - Construct a high-assurance embedded operating system for two selected embedded devices using developed tools and techniques. - Formally verify full functional correctness for selected operating systems.			

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Demonstrate required security properties that follow from correctness.			
Title: Cyber Physical Assurance and Resiliency (CYPHAR) ***Description:*** Cyber-physical systems (CPSs) are physical and engineered systems that integrate computing, communication, and storage capabilities with monitoring and/or control of entities in the physical world. CPSs are at the core of all modern weapons systems, critical infrastructure, transportation, and manufacturing environments. Due to the real-time and mission-critical nature of these systems, past and present CPS designs have focused on safety and performance with little-to-no emphasis given to resilience or assurance in the context of malicious intent. This leaves these systems vulnerable to exploitation and attack. The Cyber-Physical Assurance and Resiliency (CYPHAR) program will develop the scientific foundations that enable the design and implementation of fundamentally or highly secure systems that are capable of maintaining state awareness and an accepted level of operation in the presence of CPS threats. Scientific developments will include the definition of measures, metrics, and algorithms needed to optimize the security, safety, and performance of next generation CPS designs and will also allow for the holistic assessment of current systems in a quantitative manner. This program will develop technologies to provide provably secure protection mechanisms needed to ensure the confidentiality, integrity, and availability of system resources to support the design, testing, and implementation of highly assured and resilient CPSs. ***FY 2013 Plans:*** - Define the characteristics, measures, metrics, and associated design principles needed to build highly resilient and assured cyber physical systems (such as optimal CPS sensor distribution/placement, resiliency and assurance metrics, and latency/ response requirements). - Initiate the development of lightweight, provably secure, and highly integrated CPS sensors and encryption devices for detection and protection of combat systems. - Develop algorithms needed to autonomously create detection rule sets based on holistic CPS sensor readings.	-	-	9.000
Title: Rapid Planning (RP) ***Description:*** The Rapid Planning (RP) program will develop rapid planning and replanning tools based on recent mathematical advances. The program will develop tools and techniques for rapid generation and adaptation of robust plans in the presence of uncertainty, imprecision, incomplete, and contradictory data and assumptions. RP will also provide a capability for monitoring plans, providing continuous replanning capability, and plain text explanations for recommended plans. RP will invest in mathematical methods to improve optimization including new branch and bound, mixed integer programming, and sub-modularity methods; techniques for accelerated simulation where accuracy can be traded for speed; design of experiments through manifold learning and identification techniques that build upon previous DARPA programs; and develop a process that is aware of interdependencies in plans and aids planners in resolving these interdependencies.	5.000	9.169	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
FY 2011 Accomplishments: - Created overarching system architecture for rapid replanning incorporating environmental and tactical uncertainty. - Designed automated identifiers for the controlling and nuisance parameters to quickly focus attention. - Implemented techniques to predict optimal performance in an evolving non-linear environment. ***FY 2012 Plans:*** - Develop techniques for rapidly assessing the robustness of plans and create the ability for planners to quickly develop and deploy plan contingencies to address potential failure modes. - Demonstrate and assess the efficacy of the tool to rapidly create and adapt plans more accurately in a military laboratory environment.			
Title: Trusted Software ***Description:*** The Trusted Software program will meet DoD demands for reliable and robust software using technology to diagnose software for inefficiencies, design errors, redundant code, and overall software inconsistencies. Current software projects are massive, dynamic social efforts involving distributed teams of developers, marketers, and users. Without the proper tools, the software engineers create errors and redundancies providing unintended and exploitable security flaws. This program will develop specific techniques to extract information on software products, model the development environment, and integrate the models into low-level software analysis tools to provide a robust diagnostic tool for building and validating trustworthy software. ***FY 2011 Accomplishments:*** - Developed techniques for analyzing inter-application communication paths, including unintended paths that represent security vulnerabilities, between applications installed on a particular device. - Demonstrated feasibility of scaling the inter-application communication analysis techniques up to an apps marketplace in tests on open source apps. - Coordinated inter-application communication analysis results with potential users at NIST. ***FY 2012 Plans:*** - Demonstrate prototype software development modeling environment. - Compare, for selected software platforms, actual software behavior against intended behavior. - Analyze and determine causes of differences between actual and intended software behavior.	5.000	10.000	-
Title: Next Generation Core Optical Networks (CORONET) ***Description:*** The Next Generation Core Optical Networks (CORONET) program revolutionized the operation, performance, security, and survivability of the United States' critical inter-networking system by leveraging technology developed in DARPA photonics component and secure networking programs. Key technical enablers that were developed in this thrust include:	6.942	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
1) network management tools that guarantee optimization of high density wavelength-division-multiplexed (WDM) optical channels; 2) creation of a new class of protocols that permit the cross-layer communications needed to support quality-of-service requirements of high-priority national defense applications; and 3) demonstration of novel concepts in applications such as distributed and network-based command and control, intelligence analysis, predictive logistics management, simulation- and scenario-enhanced decision-making support for real-time combat operations, and assured operation of critical U.S. networking functions when faced with severe physical layer attack. These network-based functions support the real-time, fast-reaction operations of senior leadership, major commands and field units. ***FY 2011 Accomplishments:*** - Continued the CORONET effort to develop the network control and management software, the CORONET network-emulation testbed and the plans for technical testing and demonstrations, and formulated the technology transition plan. - Continued to work with DISA on technical oversight and evaluation of the CORONET software development effort and associated test plan. - Identified opportunities for commercial transition as well as future integration into the DISN-Core and other DoD networks.			
Title: Intrinsically Assured Mobile Ad-Hoc Networks (IAMANET) ***Description:*** The Intrinsically Assured Mobile Ad-Hoc Network (IAMANET) program completed a series of successful research programs to design a tactical wireless network that is secure and resilient to a broad range of threats which include cyber attacks, electronic warfare and malicious insiders (or captured/compromised radios). Previous programs included the Dynamic Quarantine of Computer-Based Worms (DQW) and Defense Against Cyber Attacks on Mobile Ad-hoc Network Systems (DCAMANET). IAMANET built upon the successes achieved in both the DQW and the DCMANET programs. IAMANET directly supports the integrity, availability, reliability, confidentiality, and safety of Mobile Ad-hoc Network (MANET) communications and data. In contrast, the dominant Internet paradigm is intrinsically insecure. For example, the Internet does not deny unauthorized traffic by default and therefore violates the principle of least privilege. In addition, there are no provisions for non-repudiation or accountability and therefore adversaries can probe for vulnerabilities with impunity because the likelihood of attributing bad behavior to an adversary is limited. Current protocols are not robust to purposely induced failures and malicious behavior, leaving entire Internet-based systems vulnerable in the case of defensive failure. IAMANET, on the other hand, uses a deny-by-default networking paradigm, allowing only identifiable authorized users to communicate on the network. While the objective transition path for IAMANET technologies is to the Services to support mobile tactical operations, the IAMANET systems are interoperable with fixed networks and may also have potential applicability to the broader DoD network architecture. ***FY 2011 Accomplishments:*** - Completed the design, development and integration of a secondary subsystem for the Microsoft Windows XP platform.	2.433	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Completed design and proof of concept development of trusted hardware components. - Integrated technologies into DoD's existing information assurance desktop security application Host Based Security Suite (HBSS) to enable widespread deployment.			
Title: Trustworthy Systems ***Description:*** The Trustworthy Systems program provided new approaches to network-based monitoring that provide maximum coverage of the network (i.e. from the NIPRNET/Internet gateway to service enclaves) with performance independent of the network's size, and with computational costs that either remain constant or decrease as the network's speed or relative size increases. The deliverable of this program provided network defense technologies with: (1) high probability of detection (Pd) of malicious traffic per attack launched and, (2) a false alarm rate of not more than one false alarm per day. This technology provided gateway-and-below network traffic monitoring approaches that scale at rates that are linear (or less) to increases in network size and transmission speeds. ***FY 2011 Accomplishments:*** - Developed and integrated test-case scenarios to be used in final product testing. - Completed final asymmetric routing pathway flow and traffic analysis algorithms and initiated integration into COTS high speed switching device to meet 40 Gbps speed thresholds. - Performed network testing of the 10 Gbps and 100 Gbps products.	5.731	-	-
Title: Cyber Insider Threat ***Description:*** The Cyber Insider Threat program is developing technologies for identifying advanced cyber threat missions that may be currently ongoing within DoD and government interest systems and networks. The program focuses on identifying ongoing adversary missions rather than a person, program, or particular piece of malware. Current cyber defenses are primarily based on network and host intrusion detection and look for "break-ins" and abnormal behavior without context. The CINDER program is building tools and techniques that apply mission templates of advanced cyber espionage onto seemingly normal internal system and network activity. Through this, CINDER will uncover ongoing advanced persistent cyber threats and espionage that exist within our own cyber environments. This work is continuing in PE 0603760E, Project CCC-04 beginning in FY 2012. ***FY 2011 Accomplishments:*** - Identified several areas of significant cyber insider threat currently not covered in existing technologies and capabilities. - Characterized templates for dimensions of activity, observables, and stages of existing compromises for cyber insider threat missions.	10.500	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Focused on software development lifecycle, virtual supply chains for embedded systems, and intelligence collection through persistent access.			
Accomplishments/Planned Programs Subtotals	109.608	178.419	170.642

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency			DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*	

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
IT-04: *LANGUAGE TRANSLATION*	55.047	67.015	64.408	-	64.408	72.521	71.248	51.248	51.248	Continuing	Continuing

A. Mission Description and Budget Item Justification

This project is developing powerful new technologies for processing foreign languages that will provide critical capabilities for a wide range of military and national security needs, both tactical and strategic. The technologies and systems developed in this project will enable our military to automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means. Current U.S. military operations involve close contact with a wide range of cultures and peoples. The warfighter on the ground needs hand-held, speech-to-speech translation systems that enable communication with the local population during tactical missions. Such tactical applications imply the need for two-way (foreign-language-to-English and English-to-foreign-language) translation. Because foreign-language news broadcasts, web-posted content, and captured foreign-language hard-copy documents can provide insights regarding local and regional events, attitudes, and activities, language translation systems also contribute to the development of good strategic intelligence. Such strategic applications require one-way (foreign-language-to-English) translation. Exploitation of the resulting translated content requires the capability to automatically collate, filter, synthesize, summarize, and present relevant information in near real-time.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Title: Robust Automatic Translation of Speech (RATS)	17.212	20.895	8.500

Description: The Robust Automatic Transcription of Speech (RATS) program addresses conditions in which speech signals are degraded by distortion, reverberation, and/or competing conversation. Robust speech processing technologies will enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite a noisy or reverberant environment. RATS technology will isolate and deliver pertinent information to the warfighter by detecting periods of speech activity and discarding silent portions, determining the language spoken, identifying the speaker, and recognizing key words in challenging environments.

FY 2011 Accomplishments:
- Adapted automatic speech recognition technologies to cope with highly degraded signals.
- Optimized new processing techniques for speech activity detection, language identification, speaker identification, and keyword spotting.
- Developed bio-inspired algorithms to enable RATS processing.
- Developed methods for detecting relevant speech segments.

FY 2012 Plans:
- Improve processing techniques for increasingly noisy environments, including speech activity detection, language identification, speaker identification, and keyword spotting.
- Train systems on field collected data and test systems in realistic environments.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Work with transition partners. ***FY 2013 Plans:*** - Finalize processing techniques for noisy environments, including speech activity detection, language identification, speaker identification, and keyword spotting. - Conduct final test of training systems on field collected data and test systems in realistic environments. - Transition to additional customers.			
Title: Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) ***Description:*** The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program will develop and integrate technology to enable exploitation of foreign language, hand-written documents. This technology is crucial to the warfighter, as documents including notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images captured in the field may contain extremely important time-sensitive information. The MADCAT program will address this need by producing devices that will convert such captured documents from Arabic into readable English in the field. MADCAT will substantially improve applicable technologies, in particular document analysis and optical character recognition/optical handwriting recognition. MADCAT will tightly integrate these improved technologies with translation technology and create prototypes for field trials. ***FY 2011 Accomplishments:*** - Completed the development of algorithms for interpreting different regions within a document; for predicting the syntactic structure and propositional content of text; and for removing noise from contaminated and degraded documents. - Trained and tested the technology on data collected in the field. ***FY 2012 Plans:*** - Improve translation accuracy. - Develop additional language independent and script independent technologies. ***FY 2013 Plans:*** - Transition tightly integrated technology prototypes to military and intelligence operations centers. - Train and test on larger sets of field collected data.	15.375	9.870	3.529
Title: Broad Operational Language Translation (BOLT) ***Description:*** The Broad Operational Language Translation (BOLT) program will enable communication regardless of medium (voice or text) and genre (conversation, chat, or messaging) through expansion of language translation, human-machine multimodal dialogue, and language generation capabilities. BOLT will enable warfighters and military/government personnel to readily communicate with coalition partners and local populations and will enhance intelligence through better exploitation of all	-	25.000	44.062

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
language sources including messaging and conversations. The program will also enable sophisticated search of stored language information and analysis of the information by increasing the capability of machines to perform deep language comprehension. ***FY 2012 Plans:*** - Formulate approaches for automatically processing informal genres, interpreting poor pronunciation, coping with incorrect/ incomplete syntax, resolving references, and correlating co-references. - Conceptualize approaches for comprehension of colloquialisms and idiomatic speech. - Create a fully annotated corpus of Arabic and Chinese web discussion groups. Annotation consists of translation, alignment of words between the source and target language, the grammatical structure of the sentences in both languages, and the function of the words in both languages. - Develop databases and tools to analyze Egyptian dialectal Arabic including the difference in morphology and grammar between dialectal Arabic and Modern Standard Arabic. - Enable machines to carry on multi-modal dialogues with humans and to comprehend concepts and generate responses in multilingual environments. - Enhance information retrieval and speech-to-speech translation through human-machine dialogue. - Implement paradigms for learning deep meanings of language including ability to recognize objects, manipulate them by complex commands, and reason over the objects, the commands and the environment. ***FY 2013 Plans:*** - Develop and optimize algorithms and software for processing dialectal Arabic despite the occurrence of poor pronunciation and incorrect/incomplete syntax. - Implement and evaluate initial approaches for resolving references and correlating co-references in informal communications. - Broaden approaches for translation of colloquialisms and idiomatic speech. - Enhance a fully annotated corpus of Arabic and Chinese messaging. - Develop databases and tools to analyze Levantine dialectal Arabic including the difference in morphology and grammar between dialectal Arabic and Modern Standard Arabic. - Demonstrate performance and initial capabilities for advanced algorithms and systems providing speech transcription, machine translation, and information retrieval emphasizing semantic techniques. - Evaluate early prototypes of human-machine dialogue systems with rich disambiguation capabilities. - Develop systems for human-human communication incorporating robust error detection and human-machine dialogue for correcting errors and clarifying ambiguities. - Develop initial prototypes for deep semantic acquisition of language by machines to recognize objects, manipulate them by complex commands, and reason over the objects, the commands and the environment.			
Title: Deep Extraction from Text (DEFT)	-	-	8.317

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Description: The Deep Extraction from Text (DEFT) program will enable automated extraction, processing, and inference of information from text in any application domain including technical, economic, and cultural. To accomplish this, DEFT will develop and apply formal representations for basic facts, spatial, temporal, and associative relationships, causal and process knowledge, textually entailed information, and derived relationships and correlated actions/events. DEFT inputs may be in English or in a foreign language and sources may be completely free-text or semi-structured reports, messages, documents, or data bases. DEFT will extract knowledge at scale for open source intelligence and threat analysis. Planned transition partners include the intelligence community and operational commands. ***FY 2013 Plans:*** - Develop meaning equivalence representations to relate semantically similar and equivalent texts within a document, between documents, and between documents and domain knowledge databases. - Develop methods to determine the meaning in context for words that have more than one meaning. - Design a framework to update truth values/probabilities about knowledge within and across domains. - Design methods and algorithms to infer information from multiple facts and statements. - Implement algorithms to use knowledge of the domain to answer questions and make predictions. - Develop data sets and queries for science and technology, social/cultural, and asymmetric threat domains.			
Title: Global Autonomous Language Exploitation (GALE) ***Description:*** The Global Autonomous Language Exploitation (GALE) program will create an integrated product enabling automated transcription and translation of foreign speech and text with targeted information retrieval. When applied to foreign language broadcast media and web-posted content, GALE systems will enhance open-source intelligence and local/regional situational awareness by reducing the cost and effort of translation and analysis. GALE will produce a fully-mature architecture and dramatically improve transcription and translation accuracy by broader exploitation of context. GALE will develop timely alerts for commanders and warfighters. ***FY 2011 Accomplishments:*** - Achieved high accuracy translation and distillation using shallow semantics with minimal ancillary information. - Achieved translation accuracy and distillation that exceeds human performance. - Provided technology updates to military and intelligence operations centers. ***FY 2012 Plans:*** - Support incorporation of sophisticated search capabilities developed in the distillation task of GALE into selected systems. - Transition technologies to new customers in the intelligence community and operational commands.	19.960	11.250	-
Title: Spoken Language Communication and Translation System for Tactical Use (TRANSTAC)	2.500	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Description: The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program developed technologies that enable robust, spontaneous, two-way tactical speech communications between our warfighters and native speakers. The program addressed the issues surrounding the rapid deployment of new languages, especially low-resource languages and dialects. TRANSTAC leveraged existing speech translation platforms to create a rapidly deployable language tool responsive to the military's language translation needs. ***FY 2011 Accomplishments:*** - Developed simultaneous multi-lingual translation techniques. - Demonstrated a multilingual translation prototype.			
Accomplishments/Planned Programs Subtotals	55.047	67.015	64.408

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency			DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-05: *CYBER TECHNOLOGY*	

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
IT-05: *CYBER TECHNOLOGY*	-	23.333	50.000	-	50.000	66.667	83.333	100.000	125.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Technology project supports long term national security requirements through the development and demonstration of technology to increase the security of military information systems. Over the past decade the DoD has embraced net-centric warfare to enable geographically dispersed forces to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives. This involves networking people, platforms, weapons, sensors, and decision aids to create a whole that is greater than the sum of its parts. Adversaries seek to limit this force multiplier effect through cyber attacks intended to degrade, disrupt, or deny military computing, communications, and networking systems. These cyber attacks often aim to exploit vulnerabilities and defects in military software systems. Technologies developed under the Cyber Technology project will ensure DoD cyber-capabilities survive adversary cyber attacks. Promising technologies will transition to system-level projects.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Title: Cyber Situational Awareness (CSA)*	-	10.000	21.818

Description: *Formerly Cyber Situational Awareness and Response (CSAR)

The Cyber Situational Awareness (CSA) program will develop technologies to enable comprehensive awareness and understanding of the cyber environment as required for decision-making for cyber defensive actions. This includes intelligence preparation of the cyber battlespace, indications and warning of adversary actions, detection of attack onset, attacker identification, and cyber battle damage assessment. Cyber situational awareness is made difficult by the efforts of attackers to elude detection. Approaches to cyber situational awareness will include forensic techniques to exploit data derived from events on hosts and networks that might appear innocuous when examined in isolation but reveal patterns indicative of a threat when correlated in time and space across an enterprise. CSA will also create new graphical interfaces that enable intuitive visualization of events on hosts and networks to aid in the detection of cyber attacks. This is an area where metrics are difficult to obtain, and so CSA will extend operationally-meaningful measures such as mean-time-to-detect and false-alarm rate to estimate the efficacy of proposed schemes.

FY 2012 Plans:
- Identify events on hosts and networks having the greatest potential to provide indications and warning of cyber attack.
- Conceptualize new graphical interfaces that enable intuitive visualization of anomalous events on hosts and networks suggestive of cyber attack.

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-05: *CYBER TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
- Develop canonical classes of cyber attacks and operationally-meaningful metrics to estimate the efficacy of cyber situational awareness schemes. ***FY 2013 Plans:*** - Develop and implement advanced analytic approaches and intuitive user interfaces that correlate and display events of interest in time and space across an enterprise to enable awareness of subtle intrusion attempts and persistent penetrations. - Assess the effectiveness of the cyber situational awareness techniques in detecting novel and established cyber-attacks. - Develop collaborative/interactive system concepts to enable warfighters to anticipate cyber effects and to develop cyber tactics, techniques, and procedures. - Develop and demonstrate automated algorithms/protocols that measure mission effectiveness and dynamically reconfigure network and computing resources to render attacks ineffective.			
Title: Cyber Camouflage, Concealment, and Deception (C3D) ***Description:*** The Cyber Camouflage, Concealment, and Deception (C3D) program will develop novel approaches for protecting cyber systems that mimic camouflage, concealment, and deception in the physical world. These will make attackers expend more resources to achieve their goals and provide an asymmetric advantage for the defender. C3D will enable the creation, deployment, management, and control of synthetic entities, objects, resources, and identities that produce uncertainties for attackers and make their task significantly more difficult, perhaps even intractable. With C3D, infrastructure and other enterprise resources such as switches, servers, and storage could be virtually replicated to confound enemy targeting. Decoy file systems could confuse attackers thereby greatly decreasing their odds for success. ***FY 2012 Plans:*** - Develop a framework for the creation, deployment, management, and control of synthetic entities, objects, resources, and identities on enterprise information systems. - Develop approaches for creating multiple plausible versions of file systems and data where provenance will be uncertain for the attacker. - Explore techniques capable of deceiving an attacker into believing they have executed a successful phishing attack when in fact they have been deceived by an intelligent synthetic user. ***FY 2013 Plans:*** - Demonstrate initial implementations of native and hosted synthetic object managers compatible with the most commonly used hypervisors and operating systems. - Develop techniques for protecting the synthetic object manager from detection or compromise by an attacker.	-	7.596	15.000
Title: Crowd Sourced Formal Verification (CSFV)*	-	5.737	13.182

Exhibit R-2A, RDT&E Project Justification: PB 2013 Defense Advanced Research Projects Agency		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-05: *CYBER TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2011	FY 2012	FY 2013
Description: *Formerly Crowd-Sourced Cyber in PE0601101E, Project CYS-01. The Crowd-Sourced Formal Verification (CSFV) program will develop technologies and tools to enable private citizens to participate in securing cyberspace. Private citizens already collaborate on cyber-defense through participative media dedicated to issues such as diagnosing problems on networks and remediating the effects of malware on commercial systems. CSFV will create technologies that enable crowd-sourced approaches to securing software systems through formal verification. Formal software verification is a rigorous method for proving that software has specified properties, but formal verification does not currently scale to the size of software found in modern weapon systems. CSFV will enable non-specialists to participate productively in the formal verification process by transforming formal verification problems into games that are intuitively understandable. ***FY 2012 Plans:*** - Develop approaches for mapping high-level software specifications and codes into interactive computer simulations. - Develop techniques for inferring specification and coding errors from the results of these simulations and for automatically generating the appropriate annotations. - Develop web-based infrastructure to support large scale program verification workflow. ***FY 2013 Plans:*** - Develop approaches for mapping high-level formal software verification problems into interactive computer games. - Develop techniques for inferring specification and coding errors from the solutions to these games and for automatically generating the appropriate annotations to aid formal verification. - Develop web-based infrastructure to support large scale formal software verification workflow.			
Accomplishments/Planned Programs Subtotals	-	23.333	50.000

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.