Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Defense Advanced Research Projects Agency											DATE: April 2013	
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)	**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	-	343.383	392.421	413.260	-	413.260	393.462	357.192	368.037	391.760	Continuing	Continuing
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	72.569	96.697	105.691	-	105.691	85.092	89.556	111.704	130.704	Continuing	Continuing
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	179.901	174.295	172.004	-	172.004	175.274	179.695	195.085	204.808	Continuing	Continuing
IT-04: *LANGUAGE TRANSLATION*	-	66.430	71.429	75.098	-	75.098	71.248	57.941	61.248	56.248	Continuing	Continuing
IT-05: *CYBER TECHNOLOGY*	-	24.483	50.000	60.467	-	60.467	61.848	30.000	0.000	0.000	Continuing	Continuing

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

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

A. Mission Description and Budget Item Justification

The 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 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total
Previous President's Budget	354.125	392.421	428.541	-	428.541
Current President's Budget	343.383	392.421	413.260	-	413.260
Total Adjustments	-10.742	0.000	-15.281	-	-15.281
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	-1.091	0.000			
• SBIR/STTR Transfer	-9.651	0.000			
• TotalOtherAdjustments	-	-	-15.281	-	-15.281

Change Summary Explanation

FY 2012: Decrease reflects reductions for the SBIR/STTR transfer and internal below threshold reprogrammings.

FY 2014: Decrease reflects minor repricing.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency			DATE: April 2013
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)	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
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	-	72.569	96.697	105.691	-	105.691	85.092	89.556	111.704	130.704	Continuing	Continuing

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

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

A. Mission Description and Budget Item Justification

The 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 2012	FY 2013	FY 2014
Title: META	34.000	50.000	40.691
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 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 re-programmability, 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.			
FY 2012 Accomplishments: - Matured 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Developed a domain-specific component model library for the drivetrain/mobility subsystems of a military ground vehicle through extensive characterization of desirable and spurious interactions, dynamics, and properties of all physics domains. - Developed context models to reflect various operational environments. - Developed and implemented an infrastructure for publishing and maintaining detailed component models using an ontology incorporating NATO taxonomies to expand the design space for subsequent efforts to design and build a military ground vehicle. - Developed a mechanism for the feedback of manufacturability constraints into the design and design tradespace exploration process. - Developed and integrated a library of 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 the chassis and survivability subsystems of an amphibious infantry fighting vehicle (IFV) through extensive characterization of desirable and spurious interactions, dynamics, and properties of all physics domains. - Transmit the winning design from the first Fast Adaptable Next Generation Ground (FANG) Challenge to the iFAB foundry for fabrication of an IFV drivetrain and mobility subsystem. - Begin expanded development of META tool suite to include qualitative and relational abstraction modeling, probabilistic certificate of correctness calculations, complexity metric evaluation, non-linear Partial Differential Equation (PDE) analysis and cyber design evaluation. ***FY 2014 Plans:*** - Develop domain-specific component model library for a full amphibious IFV through extensive characterization of desirable and spurious interactions, dynamics, and properties of all constituent components down to the numbered part level. - Transmit the winning design from the second FANG Challenge to the iFAB foundry to fabricate an IFV chassis and integrated survivability subsystem. - Complete development of full META tool suite necessary for the third FANG Challenge.			
Title: Instant Foundry Adaptive Through Bits (iFAB)* ***Description:*** *Formerly part of the META Program Instant Foundry Adaptive Through Bits (iFAB), will lay the groundwork for the development of a foundry-style manufacturing capability--taking as input a verified system design specified in an appropriate metalanguage--capable of rapid reconfiguration to accommodate a wide range of design variability and specifically targeted at the fabrication of military ground vehicles. The iFAB vision is to move away from wrapping a capital-intensive manufacturing facility around a single defense product, and toward the	18.000	20.000	26.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014

creation of a flexible, programmable, potentially distributed production capability able to accommodate a wide range of systems and system variants with extremely rapid reconfiguration timescales. The specific goals of the iFAB program are to rapidly design and configure manufacturing capabilities to support the fabrication of a wide array of infantry fighting vehicle models and variants. Once a given design is developed and verified, iFAB aims to take the formal META design representation and automatically configure a digitally-programmable manufacturing facility, including the selection of participating manufacturing facilities and equipment, the sequencing of the product flow and production steps, and the generation of computer-numerically-controlled (CNC) machine instruction sets as well as human instructions and training modules. iFAB is mostly an information architecture. Only the final assembly capability needs to be co-located under a single roof in anything resembling a conventional fabrication facility; the rest of iFAB can be geographically distributed and can extend across corporate and industrial boundaries, united only by a common model architecture and certain rules of behavior and business practices. The final assembly node of the iFAB facility for infantry fighting vehicles (IFV) is currently slated to be at the Joint Manufacturing and Technology Center at the Rock Island Arsenal.

FY 2012 Accomplishments:

- Began the assembly and integration of foundry-style manufacturing capability for military ground vehicles.
- Developed coarse-level determination of manufacturability time and cost for traditional and composite designs from Computer-Aided Design (CAD) models of moderate complexity.
- Created a manufacturing library describing machine tools, processes, and human capabilities for application to the Fast Adaptable Next Generation Ground (FANG) vehicle challenges.
- Developed an open source visualization of a foundry, including distributed network and assembly facility, for the verification and accurate assessment of time/accessibility/reachability for human operations within the foundry.
- Defined manufacturing requirements for drivetrain and mobility subsystem, including 140+ standard fixtures.
- Developed an open source assembly planner using collision detection tools to determine possible build sequences.
- Coordinated placement of iFAB Foundry final assembly facility at the Joint Manufacturing Technology Center at Rock Island Arsenal, IL.

FY 2013 Plans:

- Conduct a preliminary design review and critical design review (CDR) for the iFAB Foundry.
- Mature and integrate foundry infrastructure tools developed under iFAB, including manufacturing feedback and process planning.
- Develop foundry infrastructure tools to assess assembly processes and requirements.
- Upgrade the Rock Island Arsenal final assembly facility of the iFAB Foundry, and install equipment for the first FANG challenge for an amphibious IFV drivetrain and mobility subsystem.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Test process planning, manufacturing assessment and building capabilities of the distributed foundry through pre-challenges in preparation for the first FANG challenge for an IFV drivetrain and mobility subsystem. - Provide manufacturability feedback to the META design process in support of the first FANG challenge for an IFV drivetrain and mobility subsystem. - Reconfigure the iFAB foundry and build the winning drivetrain and mobility subsystem design from the first FANG Challenge. ***FY 2014 Plans:*** - Conduct a CDR for changes required within Foundry for building an IFV chassis and survivability subsystem. - Provide manufacturability feedback to the META design process in support of the second FANG challenge for an IFV chassis and survivability subsystem. - Reconfigure the iFAB foundry and build the winning chassis and survivability subsystem design from the second FANG Challenge.			
Title: Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) ***Description:*** 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 within real-world embedded system power constraints. 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 near threshold voltage operation, massive and heterogeneous processing concurrency, new architecture concepts, and 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 2012 Accomplishments:*** - Completed Ubiquitous High Performance Computing (UHPC) high level architectural designs. - Released runtime system support tools for attributing runtime costs and pinpointing system performance and stability bottlenecks. - Developed interactive compilation framework incorporating affine (linear loop parallelization) and software pipelining (find and exploit parallelization in serial codes) optimizations to automate code parallelization. - Released 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:***	15.337	26.697	35.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- 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. - Identify key language extensions and approaches required for the development of massively parallel software. ***FY 2014 Plans:*** - Develop an analytical modeling framework for fundamental design trade-off analysis and documentation for local resilience and power optimizations and global optimization methodologies and techniques. - Establish algorithmic analysis and design methodologies for power efficient and resilient processing. - Define power efficient, heterogeneous, highly concurrent conceptual architectural design approaches. - Define and evaluate the impact of 3D approaches for power efficient processing.			
Title: Adaptive Integrated Reliability	0.000	0.000	4.000
Description: The Adaptive Integrated Reliability program goals are to leverage real-time monitoring and the ability to effect fine-grained real-time control to significantly increase the lifecycle reliability of complex aerospace and defense systems. The program will also develop and demonstrate technology to reduce the incidence of catastrophic failure in complex aerospace defense systems through real-time detection and adaptation. The program will develop novel in-situ prognostication and health monitoring techniques applicable to complex air and space platforms. The program will develop tractable approaches to predict, identify, and respond to failures endemic to complex systems such as failure cascades, destructive emergent behavior, and off-nominal responses. To accomplish this, the program will leverage recent advances in adaptive control for fault isolation and mitigation. Adaptive Integrated Reliability will culminate with installation of the integrated reliability management system on a complex air or space platform and demonstrate 2X reliability improvement via accelerated lifecycle testing with representative stimuli. This reliability enhancement capability will enable development of a new generation of dependable complex systems and enable the compression of system test timelines by trading off testing for lifecycle reliability. The requisite design and production tools and techniques developed in the program will have immediate application to space systems and aircraft programs. ***FY 2014 Plans:*** - Initiate development of the integrated reliability monitoring and prediction approach to include design, analysis, processing, and appropriate sensor and platform architectures. - Initiate development of embedded sensors that possess the requisite size, energy, and environmental durability to support the Adaptive Integrated Reliability approach.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Initiate development of techniques for installation of the sensors during the platform fabrication processes.			
Title: High-Productivity Computing Systems (HPCS) ***Description:*** The High-Productivity Computing Systems (HPCS) program created a new generation of economically viable, high-productivity computing systems for the national security and industrial user communities. HPCS technologies were targeted at enabling 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 was 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 2012 Accomplishments:*** - Monitored the two HPCS performers until program completion and completed prototype demonstrations with stakeholders.	5.232	0.000	0.000
Accomplishments/Planned Programs Subtotals	72.569	96.697	105.691

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

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 2014 Defense Advanced Research Projects Agency			DATE: April 2013
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)	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
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	-	179.901	174.295	172.004	-	172.004	175.274	179.695	195.085	204.808	Continuing	Continuing

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

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

A. Mission Description and Budget Item Justification

The 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 2012	FY 2013	FY 2014
Title: Cyber Genome	24.000	15.949	5.500

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 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 2012 Accomplishments:

- Created lineage trees for a class of digital artifacts to support malware evolution forensics.
- Developed and demonstrated co-clustering and binary analysis techniques for automatically identifying re-used components in submitted malware samples.
- Created graph-based displays of malware lineage and achieved 80% accuracy on samples with known relationships.

FY 2013 Plans:

- Develop techniques to automatically and reliably extract forensically-meaningful traits such as authorship, compiler, toolkit, and obfuscation techniques.
- Enhance co-clustering and binary analysis techniques to enable the automatic identification of re-used components.
- Develop operationally relevant use case test scenarios with transition partner and conduct initial use case validation tests.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Implement prototypes incorporating the most effective techniques to transition partner specifications. ***FY 2014 Plans:*** - Demonstrate significant improvement to provenance determination through the use of the automatically extracted traits. - Demonstrate final prototypes capable of detecting a single interesting targeted threat from a stream of at least 10K uninteresting mass-infection malware samples. - Evaluate the effectiveness of prototype systems in conjunction with transition sponsors and complete transition.			
Title: Integrity Reliability Integrated CircuitS (IRIS) ***Description:*** The integrated circuit (IC) is a core component of many electronic systems developed for the Department of Defense. However, the DoD consumes a very small percentage of the total IC production in the world. As a result of the globalization of the IC marketplace, much of the advanced IC production has moved to offshore foundries, and these parts make up the majority of ICs used in today's military systems. Without the ability to influence and regulate the off-shore fabrication of ICs, there is a risk that parts acquired for DoD systems may not meet stated specifications for performance and reliability. This risk increases considerably with the proliferation of counterfeit ICs in the marketplace, as well as the potential for the introduction of malicious circuits into a design. Through the IRIS program, DARPA seeks to develop techniques that will provide system developers the ability to derive the function of digital, analog and mixed-signal ICs non-destructively, given limited operational specifications. These techniques will include advanced imaging and device recognition of deep sub-micron Complementary Metal-Oxide Semiconductor (CMOS) circuits, as well as computational methods to solve the NP-complete problem of determining device connectivity. Finally, the IRIS program will produce innovative methods of device modeling and analytic processes to determine the reliability of an IC by testing a limited number of samples. The current understanding of IC aging mechanisms, including negative bias temperature instability (NBTI), hot carrier injection (HCI), time dependent dielectric breakdown (TDDB) and electromigration (EM) will be leveraged to develop unique diagnostic test techniques. ***FY 2012 Accomplishments:*** - Completed fabrication of digital and mixed-signal IC test articles for functional derivation and reliability studies. - Completed definition of functional requirements for algorithms that determine circuit functionality without prior knowledge of their underlying logic and design. - Demonstrated the ability to resolve design features of a CMOS 90nm IC for circuit extraction through non-destructive methods. - Demonstrated functional derivation of un-altered digital and mixed-signal ICs at the 45 nm CMOS node.	30.000	18.500	6.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Demonstrated reliability derivation from reduced sample sizes of digital ICs at the 90 nm CMOS node and mixed-signal ICs at the 130 nm CMOS node. - Developed tools for functional derivation from third-party Intellectual Property (IP) blocks for both Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs). - Demonstrated the ability to observe free charges flowing in a 90 nm CMOS semiconductor device through the use of laser probing. - Demonstrated the ability to identify logic cell connections in 90 nm CMOS designs. ***FY 2013 Plans:*** - Demonstrate the ability to identify design primitives (transistors, capacitors, resistors, etc.), memory elements and interconnect through non-destructive imaging, and derive a "flattened" netlist from these components. - 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. - Develop digital and mixed-signal test articles appropriate for testing techniques for identifying unintended circuits and circuit functions. ***FY 2014 Plans:*** - Refine methods for non-destructive imaging, circuit extraction and functional derivation for improved accuracy and efficacy. - Refine methods for reliability analysis for improved accuracy, functionality and efficacy. - Encourage and support collaborative efforts among performers to develop cohesive and robust solutions for each technical thrust. - Establish advanced metrics to characterize and evaluate performer efforts for potential transition activity.			
Title: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)	29.000	28.502	28.000
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 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
FY 2012 Accomplishments: - Implemented two complete hardware tagged security processors capable of defeating common vulnerabilities and supporting novel, provably secure prototype operating systems. - Demonstrated full scale systems capable of detecting and recovering from penetrations. - Scaled automatic patch generation to more complete coverage and to work on commercial scale systems. - Automatically synthesized, using formal methods, hundreds of variants of a single distributed protocol, each of which is automatically proven correct. - Implemented a compiler that generates thousands of unique variants of programs that are demonstrated to be robust against return oriented programming attacks. - Developed a virtualization environment that provides improved security, better performance, and new functionality compared to current approaches. - Demonstrated a 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. - Transitioned CRASH network software development, retroactive patching, and code anti-tamper technologies to commercial industry.			
FY 2013 Plans: - Demonstrate moving target defense with automatically constructed diverse implementations of algorithms and programs. - Implement web-based application on secure operating systems and verify its resistance to attacks through heterogeneity. - Produce formally-verified operating system kernel modules. - Integrate tagged security processor prototypes with secure operating system, development environments for correct-by-design software, and multiple applications. - 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 into commercial router for military use.			
FY 2014 Plans: - Produce and demonstrate automation tools for constructing formally-verified operating system kernels. - Automatically produce diverse instantiations of one or more complete operating systems. - Deliver web server that enables creation of secure web sites from untrusted code. - Demonstrate real-time, continuous validation of system compliance with security specifications. - Demonstrate the ability of two or more complete systems to block, survive, and recover from multiple attacks and automatically repair vulnerabilities.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Validate security of systems and prototypes through red team and external challenges. - Transition CRASH research products into one or more embedded systems.			
Title: Safer Warfighter Computing (SAFER)	20.000	17.680	15.150

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 compute an encrypted search result without decrypting the query. This technology will advance the capability 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 2012 Accomplishments:
- Demonstrated enhanced security and availability capabilities with an order of magnitude increase in scalability and support for full web access in addition to existing applications.
- Performed initial independent, adversarial assessment of the effectiveness of SAFER technologies to prevent communication localization and detection.
- Continued development of decoy routing to support unblockable connectivity short of complete disconnection from the Internet.
- Implemented rich policy support for onion routing to enhance anonymity in the face of compromised routers.
- Performed initial, independent benchmarks of fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation.
- Computed benchmarks of the fully homomorphic encryption evaluation of the Advanced Encryption Standard demonstrating more than an order of magnitude performance improvement.
- Started design for program-wide application programming interface (API) for encrypted computation using either fully homomorphic encryption or secure multiparty computation.
- Designed program-wide API for low level mathematics to support encrypted computation using either fully homomorphic encryption or secure multiparty computation.
- Demonstrated optimized software implementations of second generation fully homomorphic encryption algorithms.

FY 2013 Plans:
- Perform follow up independent, adversarial assessment of the effectiveness of SAFER technologies to prevent communication localization and detection, including newly developed adversarial techniques.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Demonstrate field programmable gate array implementation of fully homomorphic encryption offering an order of magnitude 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. - Demonstrate two orders of magnitude improvement in performance of fully homomorphic encryption. - 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. ***FY 2014 Plans:*** - Integrate decoy routing, parallelized group messaging, dynamic traffic camouflage, and rendezvous strategy technologies into common internet browsing applications. - Demonstrate safe, anonymous internet communications applications such as web access, Voice over Internet Protocol (VOIP), and streaming video, at scale. - Conduct the final independent, adversarial assessment of the effectiveness of SAFER technologies to prevent communication localization and detection, including newly developed adversarial techniques. - Reduce ciphertext expansion while improving software performance in fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation, and perform independent benchmarks. - Refine field programmable gate array implementation of fully homomorphic encryption to yield a further order of magnitude performance improvement over optimized software implementation.			
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 2012 Accomplishments:*** - Prototyped a scalable, distributed architecture to correlate relevant data from heterogeneous sources over extended periods of time. - Formulated techniques for determining whether a system, individual, or group/organization is exhibiting anomalous behavior suggestive of a threat. - Created an experimental testbed that includes real-world data sets at scale and supports novel red-teaming capabilities.	20.000	15.000	14.612

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Initiated assessment and validation of insider-threat indicators with counter-intelligence transition partners. ***FY 2013 Plans:*** - Refine and create techniques for detecting malicious insiders, delineate assumptions/conditions under which they are valid/ invalid, and specify their effective combination. - Create a comprehensive library of test data and quantify probabilities of detection and false alarm for anomalous non-threat and threat behaviors. - Develop technologies to manage the number of anomalies, focus computing resources on ambiguous results, and prioritize threats. - Demonstrate the capability to identify anomalous behavior suggestive of a threat in real time on streaming data. ***FY 2014 Plans:*** - Develop and implement technology to capture analyst expertise for assessing and explaining detected anomalies and for incorporating such user feedback in ADAMS decision loops. - Develop an integrated prototype anomaly/threat detection system suitable for rapid deployment in an operational environment. - Harden ADAMS prototype and obtain approval for use on military networks including DOD Information Assurance Certification and Accreditation Process (DIACAP) certification. - Conduct and evaluate initial ADAMS implementation in an operational environment.			
Title: Mission-oriented Resilient Clouds* ***Description:*** *Formerly Resilient Clouds The Mission-oriented Resilient Clouds (MRC) 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. MRC 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. MRC will create new approaches to measuring trust, reaching consensus in compromised environments, and allocating resources in response to current threats and computational requirements. MRC will develop new verification and control techniques for networks embedded in clouds that must function reliably in complex adversarial environments. ***FY 2012 Accomplishments:*** - Identified algorithmic advances and protocol re-design opportunities and requirements to achieve high levels of assurance in networked/cloud computing systems. - Delivered library of new algorithms and protocols for high-assurance computation in networked/cloud computing systems.	20.389	23.500	28.071

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Developed techniques for presenting a diverse, changing target to attackers without impacting the usability of applications running on these systems. - Created approaches and algorithms for expanding self-monitoring hosts into a cooperative self-monitoring cloud. - Demonstrated new algorithms to dynamically reallocate prioritized network resources. - Implemented a new resilient microkernel on both cloud and embedded hardware platforms. - Refined cloud security requirements with DISA and focused specific projects on activities that will support future transitions into DISA and other DoD organizations. ***FY 2013 Plans:*** - Develop new behavior-based algorithms for detecting compromised machines. - Measure the effectiveness of new algorithms and protocols for high-assurance computing in cloud computing systems that are under attack. - Validate that new components are addressing resilience goals through independent red-team assessments. - Demonstrate a cloud computing environment that produces correct, mission-relevant results when individual computing and network elements have been compromised. - Develop intrusion-tolerant communication protocols for cloud monitoring and control. - Validate the extension of host-level monitoring and adaptation to cloud-level monitoring and adaptation. - Begin evaluating multiple MRC technologies in DISA testbeds to facilitate transitions into DoD clouds. ***FY 2014 Plans:*** - Produce a cloud task allocation system that maximizes mission effectiveness by employing redundancy in the context of current system loads without significantly increasing hardware costs. - Implement a trustworthy programmable switch controller. - Demonstrate dynamic adjustment of replication and communications in response to estimated and predicted attack levels. - Implement self-healing functionality for cloud applications. - Transition MRC research products into DoD cloud environments.			
Title: High Assurance Cyber Military Systems	8.250	16.064	23.117
Description: 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			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
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 Accomplishments:*** - Performed detailed requirements and systems engineering analyses to identify embedded devices requiring high assurance levels and a corresponding concept of operations. - Produced a high-level design for identified embedded computing platforms that provides a high level of assurance for military users. - Developed approaches to reduce the time to produce high-assurance embedded systems by leveraging existing high assurance systems, both through a modular architecture and through tool reuse. ***FY 2013 Plans:*** - Perform static and dynamic baseline assessments of selected militarily relevant vehicles before any modifications are made. - Develop initial techniques and build prototype tools to assist in the rapid creation of high-assurance embedded computing systems on a variety of vehicles. - Construct core pieces of a high-assurance embedded operating system and attack-resilient control system for two militarily relevant vehicles using developed tools and techniques. - Formally verify full functional correctness for core operating system and targeted control-systems for selected vehicles. - Demonstrate required security properties that follow from correctness. ***FY 2014 Plans:*** - Demonstrate compositionality which is the ability to construct high assurance systems out of high assurance components. - Extend the core high-assurance embedded operating system with additional functionality, including automatically generated device drivers and communication protocols. - Automatically synthesize correct-by-construction control systems from high-level specifications. - Perform static and dynamic assessments after modifications are made on the militarily-relevant vehicles to evaluate the effectiveness of the synthesis and formal-methods tools.			
Title: Vetting Commodity Computing Systems for the DoD* ***Description:*** *Previously part of High Assurance Cyber Military Systems	0.000	7.000	16.954

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
The Vetting Commodity Computing Systems for the DoD (VET) program will develop tools and methods to uncover backdoors and other hidden malicious functionality in the software and firmware on commodity IT devices. The international supply chain that produces the computer workstations, routers, printers, and mobile devices on which DoD depends provides many opportunities for our adversaries to insert hidden malicious functionality. VET technologies will also enable the detection of software and firmware defects and vulnerabilities that can facilitate adversary attack. ***FY 2013 Plans:*** - Create supply chain attack scenarios, formulate program analysis approaches, specify diagnostic tool functionality, develop relevant Application Programming Interfaces (APIs), and define formal semantics for the programming languages to be analyzed. - Develop the initial infrastructure required to support the development of a sufficient number of challenge programs containing hidden malicious functionality to support realistic evaluations. ***FY 2014 Plans:*** - Produce initial prototype attack scenario generation, program analysis, and diagnostic tools. - Produce initial set of challenge programs for use in the first competitive engagement. - Perform the first competitive engagement between research and adversarial challenge performers to produce measurements of research progress against program metrics.			
Title: Logan* ***Description:*** *Previously part of Cyber Fast Track The Logan program will provide DoD enhanced capabilities to conduct Computer Network Attack (CNA). Techniques will be developed to disrupt and degrade adversary information systems and network operations, with particular interest in techniques likely to be robust to adversary countermeasure strategies. ***FY 2013 Plans:*** - Formulate CNA techniques and implement in initial software routines. - Develop manual prototypes for operational transition. ***FY 2014 Plans:*** - Automate and test prototypes in conjunction with transition partner. - Optimize and harden prototypes and complete transition.	0.000	6.000	13.100
Title: Integrated Cyber Analysis System (ICAS)* ***Description:*** *Previously part of Cyber Insider Threat (CINDER) in PE 0603760E, Project CCC-04.	0.000	3.000	9.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
The Integrated Cyber Analysis System (ICAS) program will develop techniques to automate the discovery of probes, intrusions, and persistent attacks on enterprise networks. At present, discovering the actions of capable adversaries requires painstaking forensic analysis of numerous system logs by highly skilled security analysts and system administrators. The ICAS program will develop technologies to correlate interactions and behavior patterns across all system data sources and thereby rapidly uncover aberrant events and detect compromise. This includes technologies for automatically representing, indexing, and reasoning over diverse, distributed, security-related data and system files. ***FY 2013 Plans:*** - Develop techniques for transforming log/system file formats into a unified schema as the basis for an actionable view of enterprise operational security. - Develop indexing schemes specialized to system files/security data and suitable for use across federated enterprise architectures. - Develop a rigorous, quantitative, risk-management framework to serve as the basis for automated real-time network forensics and rapid detection of targeted attacks and persistent threats. ***FY 2014 Plans:*** - Develop and implement algorithms for automatically identifying and quantifying specific security risks extant on an enterprise network. - Integrate, evaluate, and optimize algorithms via testing against targeted attack/persistent threat scenarios provided by potential DoD users. - Initiate transition of the most promising technologies to enterprises throughout the DoD.			
Title: Active Cyber Defense (ACD) ***Description:*** The Active Cyber Defense (ACD) program will enable DoD cyber operators to more fully leverage their inherent home field advantage when defending the cyber battlespace. For example, in the cyber environment the defender has detailed knowledge of and unlimited access to the system resources that the attacker is attempting to compromise. ACD technologies, drawn from discoveries realized in the Cyber Fast Track program, will build on these advantages and increase the attacker's work factor by enabling cyber defenders to counter adversary cyber tradecraft in real time. ***FY 2013 Plans:*** - Formulate concepts for shaping the cyber battlespace in ways that benefit cyber defenders. - Develop approaches for countering adversary cyber tradecraft. ***FY 2014 Plans:*** - Implement techniques for countering adversary cyber tradecraft in early prototype software applications.	0.000	5.300	12.500

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Demonstrate and evaluate active cyber defense early prototypes and initial capabilities in exercises with transition partners.			
Title: Cyber Fast Track ***Description:*** 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. ***FY 2012 Accomplishments:*** - Made 77 contract awards, 22 of which have already resulted in successful field demonstrations, covering a broad range of cyber security technologies including detection and correction of software vulnerabilities, mobile device security, penetration testing automation, trust, traffic analysis, and wireless security. - Developed and demonstrated tools, methods, and techniques to reduce attack surface areas. - Refined pop-up threat list with CYBERCOM and coordinated work with other potential transition sponsors including NSA, AFRL, and the Navy Cyber Warfare Development Group. ***FY 2013 Plans:*** - Further expand outreach to additional potential customers/transition sponsors. - Complete efforts and transition technologies. - Transition of the Cyber Fast Track business model to DoD agencies.	10.000	17.800	0.000
Title: Rapid Planning (RP) ***Description:*** The Rapid Planning (RP) program developed planning and replanning tools for rapid generation and adaptation of robust plans in the presence of uncertainty, imprecision, incomplete, and contradictory data and assumptions. These enable the capability to monitor plans and continuously replan. RP addressed the need for mathematical methods to improve optimization including new branch and bound, mixed integer programming, and sub-modularity methods. ***FY 2012 Accomplishments:*** - Developed tools to facilitate various aspects of the mission planning process including formal plan representation, task sequence and timing analysis, mixed-initiative/man-machine interaction, and robust plan generation. - Created a "Mobile Task Assistant" portable workflow/collaborative planning application.	9.169	0.000	0.000
Title: Trusted Software ***Description:*** The Trusted Software program addressed 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	9.093	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
tools, the software engineers create errors and redundancies providing unintended and exploitable security flaws. This program developed specific techniques for building and validating trustworthy software. ***FY 2012 Accomplishments:*** - Developed an approach for automatically detecting and correcting integer-related vulnerabilities in source code. - Formulated a code protection technique that will provide a means to determine if an application is running in its original state or if it has been modified.			
Accomplishments/Planned Programs Subtotals	179.901	174.295	172.004

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

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 2014 Defense Advanced Research Projects Agency			DATE: April 2013
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)	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
IT-04: *LANGUAGE TRANSLATION*	-	66.430	71.429	75.098	-	75.098	71.248	57.941	61.248	56.248	Continuing	Continuing

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

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

A. Mission Description and Budget Item Justification

The Language Translation 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 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 2012	FY 2013	FY 2014
Title: Broad Operational Language Translation (BOLT)	25.907	44.062	49.729
Description: The Broad Operational Language Translation (BOLT) program will enable communication regardless of medium (voice or text) or genre (conversation, chat, or messaging) through new approaches to automated language translation, human-machine multimodal dialogue, and language generation. 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 language sources. The program will also enable sophisticated search of stored language information and analysis of the information by enabling machines to perform deep language comprehension.			
FY 2012 Accomplishments: - Developed algorithms for processing and translating the informal genres used in Arabic and Chinese internet chat by automatically analyzing and interpreting unstructured language and handling incorrect or incomplete syntax. - Created and annotated two-million word web discussion group corpora for both Arabic and Chinese including translation, word alignment, and grammatical analysis.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Developed databases, tools, and algorithms to analyze and translate Egyptian dialectal Arabic including methods to compute the differences in the lexicon, morphology, and grammar between Egyptian dialectal Arabic (used in informal settings) and Modern Standard Arabic (used in newswire and broadcasts). - Developed initial methods and algorithms for machines to perform sophisticated search of informal genres including pragmatic analysis to retrieve information and remove redundancies. - Developed the means to detect errors in automatic speech recognition (e.g., incorrect choice of homonyms) and implemented these to create robust bi-lingual human-human dialogue systems. ***FY 2013 Plans:*** - Develop improved algorithms for processing and translating informal genres of Arabic and Chinese to enable comprehension of colloquialisms and idiomatic speech in a variety of dialects. - Expand the annotated corpora of Arabic and Chinese messages by adding new dialects and enhance utility by incorporating additional annotations. - Use methods developed for Egyptian dialectal Arabic to develop databases, tools, and algorithms to analyze and translate a second Arabic dialect. - Develop improved methods and algorithms for sophisticated search of informal genres of chats and messaging including techniques to remove redundancies through entailment analysis, synonym expansion, and homonym/homograph disambiguation. - Develop enhanced automatic speech recognition techniques capable of handling errors due to the occurrence of words outside the vocabulary of the machine as well as garbled speech and integrate these into a robust bi-lingual human-human dialogue system. ***FY 2014 Plans:*** - Develop a prototype robust machine translation system for colloquial Arabic and Chinese, handling multiple genres of text, conversational speech, disfluencies, and repetitions. - Add spoken colloquial data to the Arabic and Chinese annotated corpora. - Incorporate disambiguation capabilities into a robust machine translation prototype. - Optimize methods and algorithms for sophisticated search of the informal genres of chats, messaging, and conversational speech. - Improve the accuracy and usability of systems for human-human cross-language communication by incorporating robust error detection and correction techniques in human-machine dialogue systems.			
Title: Deep Exploration and Filtering of Text (DEFT)* ***Description:*** *Formerly Deep Extraction from Text	0.000	17.946	25.369

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
The Deep Exploration and Filtering of Text (DEFT) program will enable automated extraction, processing, and inference of information from text in operationally relevant application domains. A key DEFT emphasis is to determine the implied and hidden meaning in text through probabilistic inference, anomaly detection, and disfluency analysis. 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 databases. 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 methods to derive meaning from context for words that may have implicit or hidden meanings. - Develop methods and algorithms to infer implicit information from multiple facts and statements. - Implement algorithms to use domain knowledge to discover implicit/hidden meaning, answer questions, and make predictions. - Develop data sets and queries for science and technology, human-behavioral-social-cultural, and asymmetric threat domains. ***FY 2014 Plans:*** - Develop methods and algorithms for reasoning about both explicitly and implicitly expressed opinions and beliefs. - Develop methods for finding hidden meaning based on anomalous usages and disfluencies. - Develop methods and algorithms for extracting causal and implied knowledge from a document or set of documents. - Demonstrate feasibility of deep extraction and filtering for selected end-user applications.			
Title: Robust Automatic Translation of Speech (RATS) ***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 2012 Accomplishments:*** - Improved processing techniques for increasingly noisy environments, including speech activity detection, language identification, speaker identification, and keyword spotting. - Evaluated technology on program-generated data.	20.895	7.421	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Worked with transition partners to obtain field-collected data to train and test systems in realistic environments as a precursor to transition. ***FY 2013 Plans:*** - Finalize successful processing techniques for noisy environments, including speech activity detection, language identification, speaker identification, and keyword spotting and research additional techniques. - 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 is developing and integrating 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 2012 Accomplishments:*** - Improved the accuracy of MADCAT techniques. - Developed 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. - Work with newly-collected field data.	9.870	2.000	0.000
Title: Global Autonomous Language Exploitation (GALE) ***Description:*** The Global Autonomous Language Exploitation (GALE) program created 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 enhanced open-source intelligence and local/regional situational awareness by reducing the cost and effort of translation and analysis. GALE produced a fully-mature architecture and dramatically improved transcription and translation accuracy by broader exploitation of context. GALE technology developed timely alerts for commanders and warfighters.	9.758	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
FY 2012 Accomplishments: - Supported incorporation of sophisticated search capabilities developed in the distillation task of GALE into selected systems. - Transitioned technologies to new customers in the intelligence community and operational commands.			
Accomplishments/Planned Programs Subtotals	66.430	71.429	75.098

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

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 2014 Defense Advanced Research Projects Agency			DATE: April 2013
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)	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
IT-05: *CYBER TECHNOLOGY*	-	24.483	50.000	60.467	-	60.467	61.848	30.000	0.000	0.000	Continuing	Continuing

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

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

A. Mission Description and Budget Item Justification

The Cyber Technology project develops technology to increase the security of military information systems and the effectiveness of cyber operations. Over the past decade the DoD has embraced net-centric warfare by integrating people, platforms, weapons, sensors, and decision aids. Adversaries seek to limit this force multiplier through cyber attacks intended to degrade, disrupt, or deny military computing, communications, and networking systems. Technologies developed under the Cyber Technology project will ensure DoD net-centric capabilities survive adversary cyber attacks and will enable new cyber-warfighting capabilities. Promising technologies will transition to system-level projects.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2012	FY 2013	FY 2014
Title: Foundational Cyber Warfare (Plan X)*	10.350	21.818	35.000

Description: *Formerly Cyber Situational Awareness

The Foundational Cyber Warfare (Plan X) program will develop technologies to enable comprehensive awareness and understanding of the cyber battlespace as required for visualizing, planning, and executing military cyber warfare operations. This includes intelligence preparation of the cyber battlespace, indications and warning of adversary cyber actions, detection of cyber-attack onset, cyber-attacker identification, and cyber battle damage assessment. Plan X will also create new graphical interfaces that enable intuitive visualization of events on hosts and networks to aid in the planning and execution of cyber warfare. Plan X will extend operationally meaningful measures to project quantitatively the collateral damage of executed cyber warfare missions.

FY 2012 Accomplishments:
- Conceptualized new graphical interfaces enabling intuitive visualization of the cyber battlespace.
- Created a cyber warfare domain specific language prototype.
- Developed a robust list of cyber warfare scenarios that planners may encounter.
- Prototyped a cyber warfare planning optimization and verification engine.

FY 2013 Plans:
- Finalize and implement the cyber warfare domain specific language.
- Establish a testing infrastructure to simulate a real network topology of at least 5,000 nodes.
- Deliver a Plan X version 1.0 prototype working with static network topology snapshots.
- Initiate operation of a cyber planning and operations cell with military personnel.

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- Prototype a hardened cyber weapon platform. ***FY 2014 Plans:*** - Release a Plan X version 2.0 prototype working with dynamic network topology snapshots. - Develop real-time network mapping updates and incorporate in planning and execution processes. - Finalize concept of operations for a cyber planning and operations cell. - Test on increasingly complex scenarios submitted by operational components.			
Title: Crowd Sourced Formal Verification (CSFV) ***Description:*** The Crowd-Sourced Formal Verification (CSFV) program 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 user-driven simulations that are intuitively understandable. ***FY 2012 Accomplishments:*** - Began development of approaches for mapping high-level formal software verification problems into user-driven simulations. - Identified and explored techniques for inferring specification and coding errors from the results of these simulations and for automatically generating the appropriate annotations. - Began architecture design for web-based infrastructure to support large scale program verification workflows. ***FY 2013 Plans:*** - Develop approaches for mapping high-level formal software verification problems into user-driven simulations. - Develop techniques for inferring specification and coding errors from the solutions to these simulations and for automatically generating the appropriate annotations to aid formal verification. - Develop web-based infrastructure to support large scale formal software verification workflows. ***FY 2014 Plans:*** - Develop five web-based interactive computer simulations based on mapped high-level software specifications and codes. - Launch public web site to attract the widest possible base for crowd-sourcing formal verifications. - Map solutions as code annotations back into formal verification tools and assess the effectiveness of these solutions by verifying the absence of errors on the MITRE Common Weakness Enumeration/SANS Institute Top 25 lists. - Refine initial simulations and develop new simulations for greater verification effectiveness.	6.537	13.182	20.230
Title: Cyber Warfare Control System (CWCS)	0.000	0.000	5.237

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
Description: The Cyber Warfare Control System (CWCS) program will create a semi-automated system that can sense and respond to cyber attacks more rapidly than human operators. CWCS will combine fully-automated cyber defense with man-in-the-loop cyber offense to bring to bear the full range of cyber responses allowed under applicable policies. Technologies to be developed and integrated may include anomaly detection, big data analytics, case-based reasoning, heuristics, game theory, and stochastic optimization. The CWCS capability is needed because highly-scripted, distributed cyber attacks exhibit speed, complexity, and scale that exceed the capability of human cyber defenders to respond in a timely manner. A CWCS prototype system should be capable of competing at a high level in cyber competitions. ***FY 2014 Plans:*** - Develop the high-level architecture for a semi-automated/man-in-the-loop cyber warfare control system. - Identify signals exploitable for cyber warfare and develop new instrumentation approaches for obtaining these signals. - Develop a rigorous analytic formulation for cyber warfare using techniques from game theory, stochastic optimization, and other quantitative disciplines.			
Title: Cyber Camouflage, Concealment, and Deception (C3D)	7.596	15.000	0.000
Description: The Cyber Camouflage, Concealment, and Deception (C3D) program is developing 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 Accomplishments:*** - Developed a prototype web application security platform that enables operators to embed simulated vulnerabilities into existing production websites and uses a set of match, action, and report processes to target the activities of malicious insiders. - Coordinated with network security and counter-intelligence personnel about the possibility of a pilot deployment on a particular military network. ***FY 2013 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Defense Advanced Research Projects Agency		DATE: April 2013
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 2012	FY 2013	FY 2014
- 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.			
Accomplishments/Planned Programs Subtotals	24.483	50.000	60.467

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

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