Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Defense Advanced Research Projects Agency										DATE: February 2010	
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 2009 Actual**	**FY 2010 Estimate**	**FY 2011 Base Estimate**	**FY 2011 OCO Estimate**	**FY 2011 Total Estimate**	**FY 2012 Estimate**	**FY 2013 Estimate**	**FY 2014 Estimate**	**FY 2015 Estimate**	**Cost To Complete**	**Total Cost**
Total Program Element	236.531	272.191	281.262	0.000	281.262	279.383	239.110	240.443	246.760	Continuing	Continuing
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	93.447	91.757	99.991	0.000	99.991	113.352	53.294	45.092	45.704	Continuing	Continuing
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	67.840	113.647	128.930	0.000	128.930	120.976	150.487	159.062	164.808	Continuing	Continuing
IT-04: *LANGUAGE TRANSLATION*	75.244	66.787	52.341	0.000	52.341	45.055	35.329	36.289	36.248	Continuing	Continuing

A. Mission Description and Budget Item Justification

(U) 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.

(U) The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance 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 both supercomputer and embedded computing systems.

(U) 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.

(U) 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.

B. Program Change Summary ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Previous President's Budget	250.626	282.749	0.000	0.000	0.000
Current President's Budget	236.531	272.191	281.262	0.000	281.262
Total Adjustments	-14.095	-10.558	281.262	0.000	281.262
• Congressional General Reductions		-1.140			
• Congressional Directed Reductions		-26.818			
• Congressional Rescissions	-3.854	0.000			
• Congressional Adds		2.400			
• Congressional Directed Transfers		0.000			
• Reprogrammings	-3.200	0.000			
• SBIR/STTR Transfer	-7.041	0.000			
• Congressional Restoration for New Starts	0.000	15.000	0.000	0.000	0.000
• TotalOtherAdjustments	0.000	0.000	281.262	0.000	281.262

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2009	FY 2010
Project: IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*		
Congressional Add: *High Speed Optical Interconnects for Next Generation Supercomputing*	0.000	1.200
Congressional Add Subtotals for Project: IT-02	0.000	1.200
Project: IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*		
Congressional Add: *Document Analysis and Exploitation*	1.600	0.000
Congressional Add: *Intelligent Remote Sensing for Urban Warfare*	2.400	1.200
Congressional Add Subtotals for Project: IT-03	4.000	1.200
Congressional Add Totals for all Projects	4.000	2.400

Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Defense Advanced Research Projects Agency	DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*

Change Summary Explanation

FY 2009

Decrease reflects transfer of the "National Repository of Digital Forensic Intelligence/Center for Telecommunications and Network Security" congressional add to RDT&E, Air Force account, the Section 8042 rescission of the FY 2010 Appropriation Act, SBIR/STTR transfer and internal below threshold reprogramming.

FY 2010

Decrease reflects reductions for the Section 8097 Economic Assumption, execution delays and FY 2010 new starts offset by congressional adds (as identified above) and FY 2010 Congressional Restoration for New Starts.

FY 2011

Not Applicable

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency			DATE: February 2010
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 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	93.447	91.757	99.991	0.000	99.991	113.352	53.294	45.092	45.704	Continuing	Continuing

A. Mission Description and Budget Item Justification

(U) 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 is essential for maintaining the nation's strength in both supercomputer computation for ultra large-scale engineering applications for surveillance and reconnaissance data assimilation and exploitation, and for environmental modeling and prediction.

(U) Even as this project develops the next generation of high-productivity, high-performance computing systems, it is looking further into the future to develop the technological and architectural solutions that are required to develop extreme computing systems. The military will demand increasing diversity, quantities, and complexity of sensor and other types of data, both on the battlefield and in command centers - processed in time to effectively impact warfighting decisions. Computing assets must progress dramatically to meet significantly increasing performance and cyber-security, while significantly decreasing power and size requirements. Extreme computing systems will scale to deliver a thousand times the capabilities of future petascale systems using the same power and size or will scale to deliver terascale-embedded systems at one millionth of the size and power of petascale systems, and will do so with greatly enhanced security capabilities.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
High-Productivity Computing Systems (HPCS)	65.654	51.933	30.568	0.000	30.568

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
U) The ongoing High-Productivity Computing Systems (HPCS) program will enable nuclear stockpile stewardship, weapons design, crypto-analysis, weather prediction, and other large-scale problems that cannot be addressed productively with today's computers. The goal of this multi-agency 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 programmers and scientists with minimal computer skills can harness the power of high-performance computers. The HPCS program will create a new generation of economically viable, high-productivity computing systems for the national security and industrial user communities. (U) In November 2006, the HPCS program moved into the third and final phase, with a down-select from three vendors to two. In Phase III of the HPCS program, the two remaining vendors will complete the designs and technical development of very large (petascale) productive supercomputers, with demonstration of prototype systems in 2010-2012. DARPA funding is sufficient to cover the contractual requirements of one of the two selected vendors. NSA and DOE, partners with DARPA in this program, are providing funding to maintain a second vendor in the program. *FY 2009 Accomplishments:* - Released the beta version application development software to HPCS stakeholders for evaluation and software which provided familiarity prior to system release, thus reducing the learning curve upon system availability. - Fabricated and tested several of the Application-Specific Integrated Circuits. - Continued to develop and implement operating system scaling and performance improvements. - Continued developing productivity tools. - Conducted critical design reviews of each HPCS vendor's system.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
- Began porting applications to a subset of the actual HPCS prototype hardware in preparation for FY 2010 subsystem demo that will provide evidence that the full prototype system will meet its productivity and performance goals. *FY 2010 Plans:* - Deliver final system test plan for government comment and approval. - Deliver productivity assessment report containing results of assessments to date and plans for future assessments. - Begin early subsystem demonstration of alpha or beta software running on preliminary or surrogate hardware to provide confidence that the prototype (especially hardware/software integration) is on track for FY 2011 final demonstration. - Build prototype hardware. - Integrate software onto hardware. *FY 2011 Base Plans:* - Demonstrate that the Phase III Prototype systems meet their performance and productivity commitments. - Deliver final report on Unified Parallel C (UPC) performance improvements in Symmetric Multiprocessing (SMP), Distributed and Hybrid modes that summarizes all work on UPC and demonstrates performance improvements tuned for computing hardware. - Provide the HPCS stakeholders with access to the prototype systems for a six-month evaluation and experimentation period.					
Architecture Aware Compiler Environment (AACE)* *Formerly a part of Software Producibility	10.111	10.404	13.923	0.000	13.923

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
(U) The Architecture Aware Compiler Environment (AACE) program will develop computationally efficient compilers that incorporate learning and reasoning methods to drive compiler optimizations for a broad spectrum of computing system configurations. AACE compilers will greatly simplify application development by providing the capability to automatically and efficiently generate compiled code that effectively exercises the targeted computer system resources for computer systems that range from a single, multi-core processor system to very large, multi-processor systems. The AACE program will dramatically reduce application development costs and labor; ensure that executable code is optimal, correct, and timely; enable the full capabilities of computing system advances to our warfighters; and provide superior design and performance capabilities across a broad range of military and industrial applications. *FY 2009 Accomplishments:* - Investigated initial concept for characterization tools and self-assembling compiler elements. *FY 2010 Plans:* - Demonstrate initial improved compiler approaches and characterization tools. - Perform compiler Preliminary Design Review (PDR). - Create the initial common development environment and develop supporting technologies. *FY 2011 Base Plans:* - Initiate integrated compiler and characterization environment incorporating compiler tools demonstration. - Create initial compiler environment and prototype.					
Software Producibility (U) A variety of new processor and systems architectures, including multicore and stream processors, large-scale virtualization, and the cloud computing paradigms are becoming the norm for both military	7.312	1.654	1.500	0.000	1.500

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
and civilian computing infrastructure. Unfortunately, these are highly complex technologies that exceed the capabilities of most of our programmers/application developers, and the result is that the cost of software is skyrocketing. The Software Producibility program will address this critical issue by creating technologies that reduce the cost, time, and expertise required to build large complex software systems, while ensuring that security and service guarantees are met. (U) One promising approach is an intelligent software development system that learns specific implementations of a number of high-level designs, and then uses this knowledge to create initial implementations of novel high-level designs. Automating the development of initial implementations, and then expanding this intelligence to automate debugging will save the software developer considerable time and effort. *FY 2009 Accomplishments:* - Developed tool chains to support optimized verification, field update and security adaptation experiments. - Conducted optimized verification, field update and security adaptation experiments. *FY 2010 Plans:* - Conduct load-time field update experiments. - Conduct preliminary design-time security adaptation experiments. - Conduct run-time adaptation and online run-time reconfiguration experiments. - Explore candidate demonstration systems, in addition to those used by the performer that will foster transition to the Services. - Create initial strategies for software frameworks to support multi-core, stream and cloud computing.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Develop the means to analyze and ensure the security and reliability of software created for multicore, stream and cloud computing architectures. - Create the building blocks for an intelligent development environment that offers support for sketching, gestures, and natural language as interaction modalities in a shared software design task.					
META (U) The goal of the META program is to develop novel design flows, tools, processes, and architectures to enable a significant improvement in the ability to design complex defense and aerospace systems. The program will culminate in the development and demonstration of an aircraft, ground, or naval vehicle of substantial complexity with a reduction in design, integration, manufacturing, and verification level of effort and schedule compression by a factor of five over conventional status quo approach. Likely transition partners will be the platform acquisition components of all three Services and the systems engineering community. *FY 2010 Plans:* - Develop a new model-based systems engineering process, novel design, integration, and verification flows, and appropriate supporting metrics. - Develop a modeling meta-language for the representation of models of both software and physical system components. *FY 2011 Base Plans:* - Develop supporting tools necessary to implement the model-based design, integration, and verification flows. - Using the developed tools, apply the new approach to a notional system design problem. - Determine the specific domain or domains from which the rapid development demo platform will be selected.	0.000	14.000	24.000	0.000	24.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Extreme Computing	10.370	12.566	30.000	0.000	30.000

(U) The Extreme Computing program is creating the technology base necessary for computing systems having performance that exceeds one quintillion operations per second in the post-2010 timeframe. The program is developing the specific technologies necessary for revolutionary improvements relative to scalable performance, productivity, physical size, power, programmability, data bandwidth, latency, and optimized data placement/storage. Within the context of DoD systems, mechanisms for self-modification and self-optimization will enable extreme computing systems to recognize and adapt in real-time to changing requirements, faults, malicious attacks, and opportunities to improve performance through learning. This program will develop self-aware trusted computing techniques that will provide autonomous system monitoring.

(U) The Extreme Computing program addresses several problem areas for embedded and supercomputer systems: power, programming and resiliency. Available hardware is increasingly power hungry, difficult to program, and less resilient to faults/errors. The Extreme Computing program is developing new structured architectures, tools, techniques, and an integrated design flow to enable DoD application developers to efficiently and effectively develop high-performance, mission enabling, affordable, application-specific processors. Field programmable gate arrays (FPGAs) and multi-core processors will receive particular emphasis with respect to programming issues.

FY 2009 Accomplishments:
- Performed extreme scale software study establishing framework for essential, significant changes in computing execution models.
- Analyzed existing individual design tools, identified design tool gaps, established potential approaches for a unified design development framework, and evaluated potential structured Application-Specific Integrated Circuit (ASIC) processing architecture concepts.

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2010 Plans: - Formulate new processor and memory architectures that will lead to extreme computing. - Develop initial concepts for, and evaluate the feasibility of, computational architectures and computing systems that monitor execution at run time, and dynamically optimize performance (e.g., with respect to caching, on-chip packet routing, etc.) on common applications. - Develop architectural approaches for processing time-critical applications having massive input-output requirements. *FY 2011 Base Plans:* - Develop the identified critical processor technologies, system methodologies, and architectures to enable general-purpose computing systems to perform at extreme computing levels. - Explore, develop, evaluate and perform initial simulations of techniques to enable computing systems to self-monitor their state and adapt in real time. - Perform downselects of initial extreme computing designs. - Establish initial structured ASIC architecture approaches, implement architectural test structures, and develop prototype-supporting integrated FPGA tool flow and design development environments. - Evaluate a prototype approach for large scale data storage.					
Accomplishments/Planned Programs Subtotals	93.447	90.557	99.991	0.000	99.991

	FY 2009	FY 2010
Congressional Add: High Speed Optical Interconnects for Next Generation Supercomputing *FY 2010 Plans:* Initiate research into High Speed Optical Interconnects for Next Generation Supercomputing.	0.000	1.200

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010
Congressional Adds Subtotals	0.000	1.200

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 2011 Defense Advanced Research Projects Agency			DATE: February 2010
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 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	67.840	113.647	128.930	0.000	128.930	120.976	150.487	159.062	164.808	Continuing	Continuing

A. Mission Description and Budget Item Justification

(U) This 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. The technologies will also lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites. Technologies developed under this project will be exploited by all the projects within this program element, and those 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 programs that satisfy defense requirements for secure, survivable, and network centric systems.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Next Generation Core Optical Networks (CORONET)	9.715	16.069	12.785	0.000	12.785
(U) The Next Generation Core Optical Networks (CORONET) program will revolutionize 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. These goals will be accomplished through a transformation in fundamental networking concepts that form the foundation upon which future inter-networking hardware, architecture, protocols and applications will be built. Key technical enablers that will be developed in this thrust include: 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					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
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 will support the real-time, fast-reaction operations of senior leadership, major commands and field units. (U) A complimentary effort, the Transmission, Switching and Applications for the CORONET program will develop the technology and applications to realize the next-generation dynamic multi-terabit networks that can deliver advanced internet protocol and optical services. This will be accomplished by: 1) greatly increasing network capacity through the use of more efficient fiber-optical transmission techniques; 2) implementing agile, high capacity, all optical switching platforms, and 3) developing the software and hardware interfaces, as well as the migration strategy, to enable new applications that can take full advantage of dynamic multi-terabit core optical networks. *FY 2009 Accomplishments:* Next-Generation Core Optical Networks (CORONET) - Completed the development of protocols and algorithms, and developed the network control and management architecture to provide fast service setup, fast restoration from multiple network failures and guaranteed quality of service for a global core optical network. - Modeled and simulated a dynamically reconfigurable multi-terabit global core optical network. Transmission, Switching and Applications for CORONET - Initiated the development of high-spectral efficiency banded wavelength division multiplexing (WDM) fiber-optic transmission system to enable several-fold increase in fiber capacity while providing a good match in the optical domain to the bit rate of the end user. - Architected a multi-terabit all-optical switch capable of fast switching of wavelengths and wavebands and of grooming wavelengths among wavebands.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2010 Plans: Next-Generation Core Optical Networks (CORONET) - Work with DISA to ensure that CORONET's next phase incorporates the requirements and technology evolution plan of their DISN-Core network. - Initiate the CORONET next phase development of the network control and management software and the associated test plan such that the final product will be suitable for transition and implementation in current and future commercial and DoD core optical networks. Transmission, Switching and Applications for CORONET - Complete the development and test of high-spectral efficiency banded WDM fiber-optic transmission system. - Prototype a multi-terabit all-optical switch capable of fast switching of wavelengths and wavebands and of grooming wavelengths among wavebands. *FY 2011 Base Plans:* Next-Generation Core Optical Networks (CORONET) - Continue the CORONET next phase effort to develop the network control and management software, the CORONET network-emulation testbed and the plans for technical testing and demonstrations, and complete the technology transition plan. - Continue to work with DISA on technical oversight and evaluation of the CORONET software development effort and associated test plan. - Begin developmental testing of the network control and management software on the network-emulation testbed. - Engage Standards Bodies, with the appropriate endorsements of both DISA and the commercial carrier members of the CORONET team, with the goal of amending the existing standards with the developed CORONET technology. - Pursue opportunities for commercial transition as well as future integration into the DISN-Core and other DoD networks.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Transmission, Switching and Applications for CORONET - Integrate the fiber-optic banded transmission system and the multi-terabit all-optical switch and the associated control and management software and test in a proof-of-concept test bed. - Initiate a national-scale multi-terabit network testbed to test and demonstrate hardware, software and applications of next-generation core optical networks.					
Intrinsically Assured Mobile Ad-Hoc Networks (IAMANET) (U) The Intrinsically Assured Mobile Ad-Hoc Network (IAMANET) program continues 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). (U) IAMANET will build 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.	7.432	14.543	11.912	0.000	11.912

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2009 Accomplishments: - Completed the design, development and testing of two approaches for an assurable network infrastructure (architecture, control and management, algorithms and policies). - Completed a red team evaluation of the performance of the assurable network infrastructure using a simulation of a 94 node mobile network. - Hardened DQW system against directed attacks. - Improved DQW detection and response capabilities discovered from testing. - Tested integrated DQW system on operational network. - Tested integrated DQW system against red teams (attack teams) during Combatant Command exercise. - Initiated transition of technology to DoD. *FY 2010 Plans:* - Initiate the design, development and integration of a secondary defensive subsystem (similar to what was developed under DCAMANET and the Dynamic Quarantine of Worms) for handheld devices. - Initiate design and development of trusted hardware components for specific key functions. *FY 2011 Base Plans:* - Complete the design and development of a fully integrated prototype handheld IAMANET system. - Conduct a red team test and assessment of the fully integrated prototype handheld IAMANET system. - Initiate field test and demonstrations of a medium unit set of IAMANET systems (<100 radios) in a representative operational environment.					
Trustworthy Systems (U) The goal of the Trustworthy Systems program is to provide new approaches to network-based monitoring that provide maximum coverage of the network (i.e. from the NIPRNET/Internet gateway down) with performance independent of the network's size and with computational costs that either	9.229	13.090	7.731	0.000	7.731

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
remain constant or decrease as the network's speed or relative size increases. The end deliverable of this program will provide network defense technologies with: (1) a 99% 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 will provide gateway-and-below network traffic monitoring approaches that scale at rates that are linear (or less) to increases in network size and transmission speeds. Transition partners include the National Security Agency, the Defense Information Systems Agency, and the military Services. *FY 2009 Accomplishments:* - Conducted studies on the statistical and temporal composition of prevailing traffic patterns. - Developed design architecture capable of supporting both symmetrical and asymmetrical traffic generation at speeds up to 1 Gigabite per second (Gbps). - Developed design architectures capable of generating simulated real-world traffic at network layers 2-7. - Developed traffic capturing methods in support of verifying false-positive conditions from scalable network monitoring systems being tested. - Designed a testbed that scales up to 10 Gbps, 40 Gbps, and 100 Gbps. - Designed and built 10 Gbps network monitoring devices. *FY 2010 Plans:* - Build and test a testbed that scales to traffic generation of up to 100 Gbps. - Scale a monitoring system to support line speeds of up to 100 Gbps. - Conduct a study to examine the levels of traffic fluctuation now as well as future trends. - Investigate revolutionary designs and technologies of the confident computing system, to include embedded operating systems and hypervisors. - Test network monitoring hardware at 10 Gbps and 40 Gbps.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Port system code to final hardware platform. - Test network monitoring hardware at 100 Gbps. - Transition to the agency partners listed above.					
Security-Aware Systems (U) The Security-Aware Systems program will develop and advance a variety of potentially promising technologies to enable the military to field secure, survivable, self-monitoring, self-defending network centric systems. This program will develop security aware systems that will avoid brittleness and vulnerability, due to their ability to reason about their own security attributes, capabilities and functions with respect to specific mission needs. These systems will also dynamically adapt to provide desired levels of service while minimizing risk and providing coherent explanations of the relative safety of service level alternatives. These systems will bolster the reliability and security of critical, open source software systems by reducing vulnerabilities and logic errors, and providing state-of-the-art software analysis techniques augmented with cognitive decision-making techniques with the ultimate goal of applying these systems on to the Global Information Grid. Research efforts will also explore provable protection of information within systems that exhibit imperfect security. A new kind of computational framework is needed that enables critical information and program separation properties (e.g., information in one graphical user interface (GUI) window never leaks to another GUI window). Security-Aware Systems will also address the so-called “insider threat” by developing technologies that enable a fundamentally new approach for detecting insider threats that exploits recent advances in cognitive science to accurately model and learn the normal behavior of users. (U) The Application Communities (AC) effort will develop technologies to protect DoD information systems that employ commercial software applications against cyber attack and system failure by developing collaboration-based defenses that detect, respond to, and heal from attacks with little or no human assistance. The effort will leverage advances in information assurance research programs to	9.207	11.225	12.000	0.000	12.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
create a new generation of self-defending software that automatically responds to threats, and provides a comprehensive picture of security properties, displayed at multiple levels of abstraction and formality. This capability will bring intelligent security adaptation to DoD systems, and make security properties and status more apparent to decision makers. AC technology will enable collections of similar systems to collaboratively generate a shared awareness of security vulnerabilities, vulnerability mitigation strategies, and early warnings of attack. AC will revolutionize the security of military information systems and reduce the threat from stealthy intrusion of critical systems and/or denial of service attacks. (U) The Self-Regenerative Systems (SRS) effort will design, develop, demonstrate and validate architectures, tools, and techniques for fielding systems capable of adapting to novel threats, unanticipated workloads and evolving system configurations. SRS technology will employ innovative techniques like biologically-inspired diversity, cognitive immunity and healing, granular and scalable redundancy, and higher-level functions such as reasoning, reflection and learning. SRS technologies will make critical future information systems more robust, survivable and trustworthy. SRS will also develop technologies to mitigate the insider threat. SRS-enabled systems will be able to reconstitute their full functional and performance capabilities after experiencing accidental component failure, software error, or even an intentional cyber-attack. These systems will also show a positive trend in reliability, actually exceeding initial operation capability and approaching a theoretical optimal performance level over long periods while maintaining robustness and trustworthiness attributes. *FY 2009 Accomplishments:* - Developed regimes to assess the protection mechanisms of security products, thereby providing a mechanism to certify protection to quantifiable levels based on a scientific rationale. - Developed additional general strategies to automatically immunize systems against new attacks and preempt insider attacks, enable anomaly detection, combine and correlate information from system layers, and use direct user challenges.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2010 Plans: - Employ SRS technology with a high value, mission critical, military computing system exemplar to demonstrate the system's ability to successfully complete the mission in the face of cyber attack or accidental fault. - Validate SRS technology by subjecting exemplar system to cyber attack by Red Team. - Begin the process of transition of selected self-regeneration technology to a military computing system of record. - Obtain realistic exemplars of insider threat activities. *FY 2011 Base Plans:* - Mature and evaluate technologies enabling development of a computer network that rapidly identifies, localizes and suppresses attacks and accidental faults automatically, and provides an early warning system that predicts these events. - Continue the process of transition of selected self-regeneration technology to a military computing system of record. - Use machine learning to develop rule-based models of user behavior.					
Cyber Genome* *Formerly Code Characterization. (U) Traditional cyber forensics has focused on tracing network adversaries and manual analysis of computer hosts after obtaining physical possession of the machine. Electronic evidence is fragile and can easily be modified. Additionally, cyber thieves, criminals, dishonest and even honest employees hide, wipe, disguise, cloak, encrypt and destroy evidence from storage media using a variety of freeware, shareware and commercially available utility programs. The program will develop revolutionary methods to autonomously collect, interpret and compare computer software characteristics, while mapping them against a gene-inspired construct. The program will develop	1.750	8.500	13.000	0.000	13.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
break-through cyber forensic techniques to characterize, analyze and identify malicious code. This program will also develop breakthrough abilities in visualization, threat identification analysis and threat mitigation analysis to enable positive identification of malcode sub-structures and functionality. This program will allow for the automatic discovery, identification, and characterization of any future variants of previously unknown malicious code in computing systems. *FY 2009 Accomplishments:* - Investigated revolutionary methods to autonomously extract meta data and other characteristics from multiple computing platforms. - Investigated innovative methods to determine the properties of new software code and how that code compares/contrasts to any other code. *FY 2010 Plans:* - Develop automatic techniques to rapidly and interactively reconstruct meta data to assist in the analysis of potential malicious code. - Prototype an overall system that allows for the introduction of new software code via a non-proprietary method. - Refine technologies, ontology's, and algorithms to enable the characterization of future malicious code variants based on analyzed malcode substructures. - Establish teams and community training / test data sets to evaluate the malicious code detection techniques. *FY 2011 Base Plans:* - Develop a model to determine characteristics/patterns of a user's interaction with machine hardware and software to collect signature data which can identify potential adversary users. - Complete integration of automatic discovery, identification, analysis, and prediction algorithms. - Refine user signature identification model and correlate with physical security methods.					
Trusted, Uncompromised Semiconductor Technology (TrUST)	24.507	39.020	0.000	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
(U) The Trusted, Uncompromised Semiconductor Technology (TrUST) program addresses the fundamental problem of determining whether a microchip manufactured through a process that is inherently “untrusted” (i.e., not under our control) can be “trusted” to perform operations only as specified by the design, and no more. The program will consist of a set of complementary technologies integrated together in order to develop a product that can be transitioned to the DoD. Continuation efforts are funded in the Discover program. *FY 2009 Accomplishments:* - Increased the speed of automated delayering and image processing to compare and detected changes in a fabricated IC device against the design file for a design of 10^6 transistors in 240 hours. - Increased complexity and thoroughness of Integrated Circuit (IC) design verification tools and developed methods to verify the integrity of 3rd Party Intellectual Property (IP) blocks that can work in the presence of unknown cell libraries for Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) for a design of 10^6 transistors in 240 hours. - Continued to refine and expand tools for FPGA verification and extended the number of FPGA families that they target for a design of 10^6 transistors in 240 hours. - Protected FPGAs from unauthorized substitutions by improving and empirically verifying the software/firmware framework for using Physically Unclonable Functions. *FY 2010 Plans:* - Increase the speed of automated delayering and image processing to compare and detect changes in a fabricated IC device against the design file for a design of 10^7 transistors in 120 hours. - Increase complexity and thoroughness of IC design verification tools and develop methods to verify the integrity of 3rd Party Intellectual Property (IP) blocks that can work in the presence of unknown cell libraries for ASICs and FPGAs for a design of 10^7 transistors in 120 hours. - Continue to refine and expand tools for FPGA verification and extend the number of FPGA families that they target for a design of 10^7 transistors in 120 hours.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
- Protect FPGAs from unauthorized substitutions, this will improve and empirically verify the software/ firmware framework for using Physically Unclonable Functions. - Integrate a complete TrUSTed IC solution for ASICs and FPGAs that is ready for transition. - Develop advanced IC reverse engineering techniques that can work backwards from hardware samples to derive the functionality of ICs produced with 32 nm fabrication technology. - Identify, develop, and quantify performance of innovative destructive and non-destructive evaluation techniques for 32 nm ICs which can fully evaluate the IC functionality.					
DISCOVER (U) The DISCOVER program will continue and expand the efforts initiated in TrUST, and focus on the more difficult problem of indentifying rogue components or circuitry in unknown designs. The Department of Defense has become increasingly reliant on electronic parts and systems fabricated outside of the United States. In many cases, these parts have also been designed in foreign countries, and there is currently no method available to decipher the full functionality of these circuits that may contain billions of transistors. Even if the part is designed domestically, there is currently no way of verifying that tampering has not occurred during fabrication, especially as processing technology scales to near atomic length scales. Unreliable electronic systems could potentially compromise the warfighter's mission or safety. DISCOVER will advance non-destructive reverse engineering of integrated circuits whose functionality is not known a priori. These tools will be compatible with leading edge 32 nanometer Complementary Metal-Oxide-Semiconductor (CMOS) node size. These tools will ensure that an integrated circuits has full functionality and will provide verification that no malicious changes have been introduced. *FY 2010 Plans:* - Commence definition of functional requirements for algorithms that determine circuit functionality absent knowledge of their underlying logic and design.	0.000	10.000	17.878	0.000	17.878

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Complete definition of functional requirements for algorithms that determine circuit functionality absent knowledge of their underlying logic and design. - Design tools for non-destructive interrogation of integrated circuit functionality without prior knowledge of the designed functionality.					
Cyber Authentication (U) Current practice for the authentication of military personnel to information systems and facility access uses one or more factors; something you know – passwords, something you have – access cards, and/or something you are – biometrics. Today, biometrics, a method to uniquely authenticate an individual based on one or more physical or behavior traits, relies on being able to access the individuals body (fingerprint, retina scan, face recognition, DNA) and human behavior (voice, typing rhythm) and are preferred means to identify persons. The intent of the Cyber Authentication program is to reduce the authentication burden as well as strengthening the overall network security posture of the Global Information Grid by implementing autonomous 3-factor authentication. The Cyber Authentication program will accomplish this by revolutionary non-intrusive biometric identification tied to human physiology providing autonomous network defense through consistent and non-repudiated authentication. The Cyber Authentication system will securely identify unique individuals when the individual is within proximity of a computing device. A potential transition path of this program is a commercial capability to remotely identify individuals to their commercial systems without needing to interact with today's burdensome biometric systems or remembering logon and passwords combinations. *FY 2011 Base Plans:* - Investigate revolutionary designs and technologies regarding biometric authentication utilizing micro-sensors and remote identification technologies.	0.000	0.000	5.000	0.000	5.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
- Establish an independent validation and verification team to critique performers during the design phase of the program. - Coordinate with first response community.					
Total Software Understanding (TSU)	0.000	0.000	5.000	0.000	5.000
(U) The Total Software Understanding (TSU) program seeks to develop automated tools that provide insight into the internal structure and operation of software. Current software projects are massive, dynamic social efforts involving distributed teams of developers, marketers, and users. As a result, there are multiple segments of the software being written simultaneously by different people with their own unique coding style. This segmentation of software development along with the nonstop submission of bug reports result in a continuous evolution of the system design as the software project is being developed. Over time, the software grows in size, developers phase out, and the fundamental core, structure, and layout becomes convoluted and difficult to understand. The TSU program will resolve this issue by developing software tools that distill intended software behavior and verify the intended behavior against the actual behavior. The TSU program will determine software behavior in an automated manner through low-level code analysis techniques and by examining the software development history and socio-economic impact data available during the time of development. The software tools developed under the TSU program will permit visualizations of software properties and logic flows as well as allow a historical and performance analysis of those properties. TSU will enable software engineers to diagnose software for inefficiencies, logic errors, redundant code, and overall software inconsistencies. The tools developed under the TSU program will permit automated software restructuring for efficiency. The ultimate goal of the TSU program is to build tools that enable software developers to improve the overall quality of current and future software products. The software tools developed in this program will enable the improvement and modernization of legacy and open source software, as well as improve and guide future software engineering practices and techniques. This effort will transition to the Department of Defense (DoD) agencies, Military Services, academic, and commercial sectors.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Develop models from historical, socio-economic data, and software builds for analysis. - Develop tools to perform historical analysis of software builds/releases over time. - Develop tools to analyze models for intended behavior.					
Confident Computing (C-2) (U) The Confident Computing (C-2) program will radically change the current paradigm of overly complex, unwieldy, and insecure computing platforms. Current commercial off-the-shelf (COTS) systems do not keep pace with the security requirements of the Department of Defense and other government agencies; they are incentivized to add layer upon layer of functionality and backwards compatibility, without significantly improved security. The C-2 program will leverage enhanced processor and memory technologies developed under the Trustworthy Systems program to revolutionize the “minimalization” of a micro-core operating system, designed to quantifiably defeat adversaries’ attempts to compromise the system during computing operations specific to military operations, rather than home use. The resulting technology of the C-2 program will initially be used either as a component or complete system to allow secure command and control communications for deployed forces. Subsequent phases of the program will allow for expanded usability and functionality for in-garrison usage. Mature C-2 technologies will not require add-on security controls (e.g., Anti-Virus, Firewall, etc.) nor time-consuming maintenance from system administrators, thus improving performance and decreasing costs in order to facilitate transition to an operational performer. *FY 2011 Base Plans:* - Investigate revolutionary designs and technologies of the C-2 system, including embedded operating systems and hypervisors. - Develop technology via approved software development life cycle approach. - Establish an independent validation and verification team to critique the performers during the design phase of the technologies.	0.000	0.000	5.349	0.000	5.349

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Securing the Hosts	0.000	0.000	9.275	0.000	9.275
(U) The Securing the Hosts program will meet the steadily increasing DoD demands for a new computing infrastructure with a much higher level of security. Securing the Hosts will create new, safer, computer languages and compilers; formal automated proof tools and development environment for security throughout the execution model; and techniques for design and pre-run-time validation of executables. The Securing the Hosts program will take a clean slate approach to the execution model; executables will be crypto-bound to the lower levels of the execution model, subject to proofs checks, and constructed with security-aware languages. Technical approaches will include, but are not limited to co-development of hardware and low level system software, with cryptographic microcontrollers to permit cryptographic handshaking at all system layers; lower levels of the execution model establish a root of trust from the hardware out through the hypervisor and other secure low-level software, cryptographically bound to the upper levels of the execution model; novel hardware architectures for data-provenance tracking, access rights enforcement, information flow tracking and tagging, cryptography, logic, memory, and data access to support secure execution; and provably secure hypervisor. *FY 2011 Base Plans:* - Develop concepts for a clean-slate re-design of the upper portion of the execution model, including the programming model, compiler, libraries, run time, and operating system. - Develop concepts for a clean-slate re-design of the upper portion of the execution model, including virtual machines, the micro operating system, hardware abstraction layer, hypervisor, CPU, and crypto microcontroller. - Create concepts for co-design of the execution model, hardware and verification technologies to ease proofs and dynamic enforcement of security properties. - Create initial implementations for new, provably-secure elements of the execution model. - Develop concepts and initial implementations for providing arbitrary computation on encrypted data.					
Securing the Network	0.000	0.000	9.000	0.000	9.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
(U) The Securing the Network program will meet the steadily increasing DoD demands for a new networking infrastructure with a much higher level of security. Clean slate architectures for Internet protocols are needed that reflect security and trust explicitly in their design, starting with network and transport functions, to derive far greater roots of trust. Protocols that reflect more compute intensive approaches to control are enabled by the drastic reduction of computing cost, compared to design assumptions decades ago. Specific approaches will include, but are not limited to, cryptographic handshake at all network layers above physical and data link functions; network management software that exhibits strong roots of trust, running in trusted substrates; routers that permit significant computing power to be applied at intermediate points along the data pathways and provide virtualization features enabling multiple protocols to be deployed; and information movement based on object-by-object encryption, with accountability enforced in network appliances at all network levels. *FY 2011 Base Plans:* - Develop concepts for a clean-slate re-design of Internet protocols that reflect security and trust explicitly in their design, starting with layer 3 and 4 protocols (network and transport functions). - Develop concepts for an accountable cyberinfrastructure in which it is possible to trace flows to establish the provenance, and by implication the trustworthiness, of network data and information. - Create initial designs for Internet protocols that reflect security and trust explicitly in their design, starting with layer 3 and 4 protocols (network and transport functions). - Develop initial implementations for highly available, censorship-resistant network infrastructure.					
Rapid Planning (RP) (U) The Rapid Planning (RP) effort will develop rapid planning and replanning tools based on a mathematical foundation. 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	0.000	0.000	5.000	0.000	5.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
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. *FY 2011 Base Plans:* - Create overarching system architecture for rapid replanning incorporating environmental and tactical uncertainty. - Design automated identification of the controlling and nuisance parameters to control accuracy.					
Cyber Immune (U) Cyber security is one of the top challenges facing the DoD and the nation. Despite many years of research in this area, the security of the Internet and our computing systems continues to be insufficient to support the degree of dependence that is increasingly vested in this infrastructure by the military and industry. At the same time, in several other areas such as robotics, DARPA has made significant new breakthroughs by using the mechanisms of biological systems as inspiration for radical re-thinking of basic hardware and system designs. This project seeks to accomplish the same in the cyber-security area. It will investigate and develop new approaches to cyber-security inspired by biological systems, in order to gain major improvements. Higher levels of system security will come from new biologically inspired models that will replace the failed model of perimeter defense that currently dominates today's information systems. This project will develop cyber-resilient systems that assume security cannot be absolute, yet a system that can still defend itself in order to maintain its (possibly degraded) capabilities, and possibly even heal itself. *FY 2011 Base Plans:* - Develop new models of software that enable systems to detect the presence of cyber-attack agents.	0.000	0.000	15.000	0.000	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
- Create new techniques for software systems to garner its resources for cyber-defense while still maintaining some of its operating capabilities. - Develop initial concepts for methods of warding off attacks and, when possible, healing the system.					
Control-Based Mobile Ad-Hoc Networks (CBMANET) (U) The Control-Based Mobile Ad-Hoc Networks (CBMANET) program developed an adaptive networking capability that dramatically improved performance and reduced life-threatening communication failures in complex communication networks. The program focused on tactical mobile ad-hoc networks (MANETs) that were inadequately supported with commercial technology. To address this problem, the CBMANET program exploited recent optimization-theoretic breakthroughs, recent information-theoretic breakthroughs, and comprehensive cross-layer design to develop a network stack from first principles with specific attention to support for DoD applications such as multicast voice video, chat, file transfer, and situation awareness. *FY 2009 Accomplishments:* - Completed development and integration into military radio systems. - Executed final experiments and military demonstrations. - Transitioned activities to the Services.	2.000	0.000	0.000	0.000	0.000
Accomplishments/Planned Programs Subtotals	63.840	112.447	128.930	0.000	128.930

	FY 2009	FY 2010
Congressional Add: Document Analysis and Exploitation *FY 2009 Accomplishments:* - Conducted research in document analysis and exploitation.	1.600	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010
Congressional Add: Intelligent Remote Sensing for Urban Warfare *FY 2009 Accomplishments:* - Conducted research in remote sensing for urban warfare. *FY 2010 Plans:* - Continue to conduct research in remote sensing for urban warfare operations.	2.400	1.200
Congressional Adds Subtotals	4.000	1.200

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 2011 Defense Advanced Research Projects Agency			DATE: February 2010
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 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
IT-04: *LANGUAGE TRANSLATION*	75.244	66.787	52.341	0.000	52.341	45.055	35.329	36.289	36.248	Continuing	Continuing

A. Mission Description and Budget Item Justification

(U) 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.

(U) 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. Thus, tactical applications imply the need for two-way (foreign-language-to-English and English-to-foreign-language) translation.

(U) 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 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 timely and relevant forms.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Spoken Language Communication and Translation System for Tactical Use (TRANSTAC)	11.533	7.738	2.500	0.000	2.500
(U) The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program is developing technologies that enable robust, spontaneous, two-way tactical speech communications between our warfighters and native speakers. The program addresses the issues surrounding the rapid deployment of new languages, especially low-resource languages and dialects. TRANSTAC is building upon existing speech translation platforms to create a rapidly deployable					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
language tool that will meet the military's language translation needs. TRANSTAC is currently focusing on key languages of the Middle East region. *FY 2009 Accomplishments:* - Updated/enhanced the experimental systems in the field. - Continued mission needs analysis and aggressive language data collection. - Developed an initial Dari prototype that will undergo further testing. *FY 2010 Plans:* - Test and refine the Dari prototype. - Develop context management translation techniques. - Demonstrate a hands-free, eyes-free, two-way translator prototype. - Extend translation techniques to develop translation systems emphasizing other key languages (e.g., Pashto). *FY 2011 Base Plans:* - Develop simultaneous multi-lingual translation techniques. - Demonstrate a multilingual translation prototype. - Test translation systems emphasizing other key languages.					
Global Autonomous Language Exploitation (GALE) (U) The Global Autonomous Language Exploitation (GALE) program will provide, in an integrated product, automated transcription and translation of foreign speech and text along with content summarization. When applied to foreign language broadcast media and web-posted content, GALE systems will enhance open-source intelligence and local/regional situational awareness and eliminate the need for translation and subject matter experts. Continuing work under GALE will produce a fully mature integrated architecture and dramatically improve transcription and translation accuracy by exploiting context and other clues. GALE will address unstructured speech such as talk show	46.396	37.353	22.945	0.000	22.945

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
conversations and chat room communications, developing timely, succinct reports and alerts for commanders and warfighters. *FY 2009 Accomplishments:* - Incorporated syntactic analysis of the source languages (Arabic and Chinese) and developed more accurate word alignment between source and target languages. - Performed design and feasibility experiments for extraction-empowered machine translation, where the system extracts the meaningful phrases (e.g., names and descriptions) from foreign language text for highly accurate translation into English. - Analyzed English sentences (original or translated) in terms of the editorial 5W's (Who, What, Where, When and Why) and designed methods for evaluating the results. - Continued transitioning preliminary technologies developed by the GALE program into high-impact military systems and intelligence operations centers. *FY 2010 Plans:* - Develop methods for porting technology into new languages. - Complete the architecture for a summarization system that incorporates adaptive filtering, focused summarization, information extraction, contradiction detection, and user modeling. - Continue incorporating predicate-argument analysis to enhance machine translation and summarization. - Develop methods for using extraction-empowered machine translation, where the system extracts the meaningful phrases (e.g., names and descriptions) from foreign language text for highly accurate translation into English. - Continue to transition technologies developed by the GALE program into high-impact military systems and intelligence operations centers. - Exercise language independent paradigm for new languages essential for military use - Dari, Pashto and Urdu.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Continue improvement of transcription and translation algorithms, use of shallow semantics to achieve high accuracy translation and distillation, and evaluation of translation and distillation technologies. - Achieve the ultimate GALE targets of ninety-five percent translation accuracy and distillation that exceeds human performance. - Continue to transition technologies developed by the GALE program into high-impact military systems and intelligence operations centers. - Continue development of Dari, Pashto and Urdu in addition to GALE languages of Arabic and Chinese translation.					
Multilingual Automatic Document Classification, Analysis and Translation (MADCAT)	12.639	13.500	15.375	0.000	15.375
(U) The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program will develop and integrate technology to enable exploitation of captured, foreign language, hard-copy documents. This technology is crucial to the warfighter, as hard-copy documents including notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images (e.g., PDF files, JPEG files, scanned TIFF images, etc.) resident on magnetic and optical media captured in the field may contain important, but perishable information. Unfortunately, due to limited human resources and the immature state of applicable technology, the Services lack the ability to exploit in a timely fashion ideographic and script documents that are either machine printed or handwritten in Arabic. The MADCAT program will address this need by producing devices that will convert such captured documents to readable English in the field. MADCAT will substantially improve the applicable technologies, in particular document analysis and optical character recognition/optical handwriting recognition (OCR/OHR). MADCAT will then tightly integrate these improved technologies with translation technology and create demonstration prototypes for field trials.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2009 Accomplishments: - Continued improving methods for document segmentation (e.g., title, address box, columns, lists, embedded picture/diagram/caption, annotation, signature block, etc.). - Developed improved algorithms for document type identification (e.g., letter, ledger, annotated map, newspaper, etc.) for discrimination and separation of handwriting from printed regions; and for improved OCR/OHR. - Created better means of interpreting different regions within a document such as extracting information from an address field or the axes of a table. - Developed algorithms to predict the syntactic structure and propositional content of text, and for recognizing and transcribing hand-written text. - Integrated these improvements with the translation component of GALE to yield tightly integrated technology prototypes that convert captured documents into readable and searchable English. - Enabled efficient metadata-based search and retrieval. *FY 2010 Plans:* - Develop optimized algorithms for interpreting different regions within a document, such as extracting information from an address field or the axes of a table; for predicting the syntactic structure and propositional content of text; and for removing noise from contaminated and degraded documents. - Integrate these improvements with the translation and summarization components of GALE to yield tightly integrated technology prototypes that convert captured documents into readable and searchable English. - Transition tightly integrated technology prototypes to high-impact military systems and intelligence operations centers. - Extend language independent technology to languages also using Arabic script - Dari, Pashto and Urdu.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: - Complete the development and optimization of algorithms for interpreting different regions within a document, such as extracting information from an address field or the axes of a table; for predicting the syntactic structure and propositional content of text; and for removing noise from contaminated and degraded documents. - Complete the integration of these improvements with the translation and summarization components of GALE. - Transition tightly integrated technology prototypes that convert captured documents into readable and searchable English to high-impact military systems and intelligence operations centers. - Continue development of language independent technology extension to Dari, Pashto and Urdu.					
Robust Automatic Translation of Speech (RATS) (U) The Robust Automatic Translation of Speech (RATS) program will address noisy and hostile conditions where speech is degraded by distortion, reverberation, and/or competing conversations. Research into the issue of robustness to enhance the capabilities of speech processing will enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite a noisy or echoic environment. In extremely noisy conditions, the technology developed through RATS will be able to isolate and deliver pertinent information to the warfighter by detecting periods of speech activity and discarding silent portions. RATS technology will also be able to detect the language spoken, identify the speaker, and search for key words in dialogue. RATS technology will build upon advances in GALE translation technology. *FY 2009 Accomplishments:* - Evaluated the relative benefits (performance versus computational requirements) of noise suppression and speech exploitation based on a single microphone versus using a dual-microphone.	4.676	8.196	11.521	0.000	11.521

Exhibit R-2A, RDT&E Project Justification: PB 2011 Defense Advanced Research Projects Agency		DATE: February 2010
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 Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
- Assessed the current state of the art in speech processing for noisy environments, including echo suppression, speech activity detection, language identification, speaker identification and keyword spotting. *FY 2010 Plans:* - Develop robust automatic speech transcription and translation algorithms for use in adverse environments (those with noise, distortion, reverberation, and/or competing speech signals). - Develop noise suppression and speech exploitation based on multi-microphone arrays. - Refine new speech processing techniques for noisy environments, including echo suppression, speech activity detection, language identification, speaker identification and keyword spotting. *FY 2011 Base Plans:* - Optimize new speech processing techniques for noisy environments, including echo suppression, speech activity detection, language identification, speaker identification and keyword spotting. - Plan for transition of technologies developed through RATS into high-impact military systems and intelligence operations centers.					
Accomplishments/Planned Programs Subtotals	75.244	66.787	52.341	0.000	52.341

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.