

**UNCLASSIFIED**

**Exhibit R-2, PB 2010 Defense Advanced Research Projects Agency RDT&E Budget Item Justification** **DATE:** May 2009

<b>APPROPRIATION/BUDGET ACTIVITY</b>					<b>R-1 ITEM NOMENCLATURE</b>					
0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research					PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY					
<b>COST (\$ in Millions)</b>	<b>FY 2008 Actual</b>	<b>FY 2009 Estimate</b>	<b>FY 2010 Estimate</b>	<b>FY 2011 Estimate</b>	<b>FY 2012 Estimate</b>	<b>FY 2013 Estimate</b>	<b>FY 2014 Estimate</b>	<b>FY 2015 Estimate</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
Total Program Element	184.664	250.626	282.749						Continuing	Continuing
IT-02: HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES	56.913	98.641	96.991						Continuing	Continuing
IT-03: INFORMATION ASSURANCE AND SURVIVABILITY	61.621	76.966	113.587						Continuing	Continuing
IT-04: LANGUAGE TRANSLATION	66.130	75.019	72.171						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

**UNCLASSIFIED**

R-1 Line Item #11

Page 1 of 32

**UNCLASSIFIED**

**Exhibit R-2, PB 2010 Defense Advanced Research Projects Agency RDT&E Budget Item Justification** **DATE:** May 2009

<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY
---	---

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)**

	<b><u>FY 2008</u></b>	<b><u>FY 2009</u></b>	<b><u>FY 2010</u></b>	<b><u>FY 2011</u></b>
Previous President's Budget	230.385	254.009	234.676	
Current BES/President's Budget	184.664	250.626	282.749	
Total Adjustments	-45.721	-3.383	48.073	
Congressional Program Reductions	0.000	-8.583		
Congressional Rescissions	-14.000	0.000		
Total Congressional Increases	0.000	5.200		
Total Reprogrammings	-25.413	0.000		
SBIR/STTR Transfer	-6.308	0.000		
TotalOtherAdjustments			48.073	

**Congressional Increase Details (\$ in Millions)**

**Project: IT-03, Document Analysis and Exploitation**

**Project: IT-03, Intelligent Remote Sensing for Urban Warfare Operations**

**Project: IT-03, National Repository of Digital Forensic Intelligence/Center for Telecommunications and Network Security**

	<b>FY 2008</b>	<b>FY 2009</b>
Project: IT-03, Document Analysis and Exploitation	0.000	1.600
Project: IT-03, Intelligent Remote Sensing for Urban Warfare Operations	0.000	2.400
Project: IT-03, National Repository of Digital Forensic Intelligence/Center for Telecommunications and Network Security	0.000	1.200

**Change Summary Explanation**

FY 2008

Decrease reflects the Section 8042 rescission, the OSD AFRICOM and O&M reprogrammings, below threshold reprogramming actions and the SBIR/STTR transfer.

FY 2009

Decrease reflects reductions for Section 8101 Economic Assumptions offset by congressional adds (as identified above) and congressional reductions.

FY 2010

Increases reflect additional funds in the High Productivity, High Responsive Architectures project for new architecture programs and increased emphasis on Information Assurance programs.

**UNCLASSIFIED**

R-1 Line Item #11

Page 2 of 32

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>								<b>DATE:</b> May 2009		
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research				<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY					<b>PROJECT NUMBER</b> IT-02	
<b>COST (\$ in Millions)</b>	<b>FY 2008 Actual</b>	<b>FY 2009 Estimate</b>	<b>FY 2010 Estimate</b>	<b>FY 2011 Estimate</b>	<b>FY 2012 Estimate</b>	<b>FY 2013 Estimate</b>	<b>FY 2014 Estimate</b>	<b>FY 2015 Estimate</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
IT-02: HIGH PRODUCTIVITY, HIGH- PERFORMANCE RESPONSIVE ARCHITECTURES	56.913	98.641	96.991						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 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. The resulting extreme computing systems will be capable of scaling from embedded to leadership class supercomputer systems. The most significant technical achievements that must be realized to obtain the goals of extreme computing are the enabling architectural advancements, pervasive low power approaches, low volume physical packaging, and effective programming of these systems. Numerous additional technical challenges must be resolved, including the reliability of "extreme computing" systems: embedded systems require a higher level of reliability and assurance than general-purpose systems because the failure of an embedded computing system can result in the loss of a deployed platform.

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-02	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>High-Productivity Computing Systems (HPCS)</p> <p>(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.</p> <p>(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.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Completed design verification of some application-specific integrated circuits (ASICs), a critical step before releasing design to the very costly fabrication process.</li> <li>- Developed and implemented operating system scaling and performance improvements so that existing operating systems can be leveraged, saving development costs, facilitating use of legacy code, and improving user productivity by preventing the need to learn a new operating system.</li> <li>- Continued developing productivity tools and demonstrated early versions of productivity tools for the HPCS stakeholders to solicit their feedback.</li> <li>- Conducted an HPCS software critical design review of each vendor.</li> <li>- Evaluated vendor delivered design specifications.</li> <li>- Explored opportunities to expand the user base for high-end computing.</li> </ul>	43.243	71.654	60.904	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-02	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Release the beta version application development software to HPCS stakeholders for evaluation and to provide familiarity with the software prior to system release thus reducing the learning curve upon system availability.</li> <li>- Fabricate and test several of the ASICs.</li> <li>- Continue to develop and implement operating system scaling and performance improvements.</li> <li>- Continue developing productivity tools.</li> <li>- Conduct critical design review of each HPCS vendor's system.</li> <li>- Begin 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.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Deliver final system test plan for government comment and approval.</li> <li>- Deliver productivity assessment report containing results of assessments to date and plans for future assessments.</li> <li>- Begin early subsystem demonstration of alpha or beta software running on preliminary or surrogate hardware which provides confidence that the prototype (especially hardware/software integration) is on track for FY 2011 final demonstration.</li> <li>- Build out prototype hardware.</li> <li>- Integrate software onto hardware.</li> </ul>				
<p>Software Producibility</p> <p>(U) The Software Producibility program will reduce the cost, time, and expertise required to build large complex software systems. This includes new techniques for rapidly developing adaptive software that can be easily changed to conform to new software design and development tools, readily complies with new requirements, and readjusts dynamically to environmental perturbation. Improvements in compiler technology can greatly simplify application development by providing the capability to automatically and efficiently generate compiled code that effectively exercises the targeted computer system resources for a broad spectrum of military and industrial applications, and for computer systems that range from a single,</p>	7.600	15.996	22.087	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-02	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>multi-core processor system to very large, multi-processor systems. Significant advances in software development technology will be made as new processor technologies such as multicore, stream, and the cloud computing paradigms become the norm for both military and civilian computing infrastructure. Security and service guarantees will be addressed.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed tool chains to support preliminary flight control/vehicle management system and software-defined radio experiments.</li> <li>- Conducted a fault management design time experiment.</li> <li>- Conducted software-defined radio design-time and load-time adaptation experiments.</li> <li>- Investigated initial community-based concepts for characterization tools and self-assembling compiler elements.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop tool chains to support optimized verification, field update and security adaptation experiments.</li> <li>- Conduct optimized verification, field update and security adaptation experiments.</li> <li>- Investigate initial concept for characterization tools and self-assembling compiler elements.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Conduct load-time field update experiments.</li> <li>- Conduct preliminary design-time security adaptation experiments.</li> <li>- Conduct run-time adaptation and online run-time reconfiguration experiments.</li> <li>- Create the initial common development environment and develop supporting technologies.</li> <li>- Demonstrate initial improved compiler approaches and characterization tools.</li> <li>- Create initial strategies for software frameworks to support multi-core, stream and cloud computing.</li> </ul>				
<p>Extreme Computing</p> <p>(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</p>	6.070	10.991	14.000	

**UNCLASSIFIED**

R-1 Line Item #11

Page 6 of 32

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-02	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>scalable performance, productivity, physical size, power, programmability, data bandwidth, latency, and optimized data placement/storage. This includes creating the new Dynamic Random Access Memory (DRAM) architectural approaches that are essential if overall memory performance is to keep up with processor performance. Such DRAM improvements and other architectural breakthroughs are essential for processing time-critical applications having massive input-output requirements. 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.</p> <p>(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.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Identified and assessed the potential technologies necessary to provide the types of improvements essential to achieve extreme computing: non-von Neumann architectures; 3-D microelectronic structures; high-bandwidth/low-latency electrical and optical technologies; multiple-core processors; radically different packaging solutions; new memory and storage architectures; and non-intrusive interfaces.</li> <li>- Initiated a study to identify potential new hardware architectures and candidate approaches, such as master/slave methods where the "slave" collects and condenses data.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Investigate new memory architecture approaches that overcome the limitations of current DRAM.</li> <li>- Formulate new processor and memory architectures that will lead to extreme computing.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009		
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-02		
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>	
<ul style="list-style-type: none"> <li>- Analyze existing individual design tools, identify design tool gaps, establish approaches for a unified design development framework, and evaluate potential structured Application-Specific Integrated Circuit (ASIC) processing architecture concepts.</li> <li>- 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.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop new memory architecture approaches, develop enabling prototype critical memory and memory module technologies.</li> <li>- Develop the identified critical and processor technologies, system methodologies, and architectures to enable general-purpose computing systems to perform at extreme computing levels.</li> <li>- Develop the approaches, frameworks, initial architectural concepts and tool implementations essential to implement structured ASIC processing architectures and integrated application development environments.</li> <li>- Explore, develop, evaluate and perform initial simulations of techniques to enable computing systems to self-monitor their state and adapt in real time.</li> <li>- Develop architectural approaches for processing time-critical applications having massive input-output requirements.</li> </ul>					
<b>C. Other Program Funding Summary (\$ in Millions)</b>					
N/A					
<b>D. Acquisition Strategy</b>					
N/A					
<b>E. Performance Metrics</b>					
Specific programmatic performance metrics are listed above in the program accomplishments and plans section.					

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>								<b>DATE:</b> May 2009		
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research				<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY					<b>PROJECT NUMBER</b> IT-03	
<b>COST (\$ in Millions)</b>	<b>FY 2008 Actual</b>	<b>FY 2009 Estimate</b>	<b>FY 2010 Estimate</b>	<b>FY 2011 Estimate</b>	<b>FY 2012 Estimate</b>	<b>FY 2013 Estimate</b>	<b>FY 2014 Estimate</b>	<b>FY 2015 Estimate</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
IT-03: INFORMATION ASSURANCE AND SURVIVABILITY	61.621	76.966	113.587						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)**

	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>Next Generation Core Optical Networks (CORONET)</p> <p>(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, such as those provided by wavelength division multiplexing; 2) creation of a new class of protocols that permit the cross-layer communications needed to support quality-of-service requirements of high-priority national defense applications; and 3) demonstration of novel concepts in applications such as distributed and network based command and control, intelligence analysis, predictive logistics management, simulation and scenario enhanced decision-making support for real-time combat operations, and assured operation of critical U.S. networking functions when faced with severe physical layer attack. These network-based</p>	13.520	13.200	16.069	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>functions will support the real-time, fast-reaction operations of senior leadership, major commands and field units.</p> <p>(U) A complimentary effort, the Transmission, Switching and Applications for Next-Generation Core Optical Networks (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.</p> <p><i>FY 2008 Accomplishments:</i>            Next-Generation Core Optical Networks (CORONET)            - Established a common global core optical network topology.            - Developed the architectures and defined the network elements for a fast reconfigurable optical core network.            - Initiated development of protocols and algorithms to provide fast service setup, fast restoration from multiple network failures and guaranteed quality of service for a global core optical network.</p> <p>Transmission, Switching and Applications for CORONET            - Completed a study on how to increase the spectral efficiency of existing optical networks by up to ten times.            - Completed a study to determine the impacts of emerging 100 Gbps Ethernet technology on next-generation optical networks.            - Initiated a study to examine migration strategies and associated software and hardware interfaces to enable new applications for next-generation core optical networks.            - Initiated a study of banded vs. channelized wavelength division multiplexing (WDM) transmission in spectrally efficient fiber-optic links.</p>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p><i>FY 2009 Plans:</i>            Next-Generation Core Optical Networks (CORONET)            - Complete the development of protocols and algorithms, and develop 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.            - Model and simulate a dynamically reconfigurable multi-terabit global core optical network.</p> <p>Transmission, Switching and Applications for CORONET            - Initiate 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.            - Architect a multi-terabit all-optical switch capable of fast switching of wavelengths and wavebands and of grooming wavelengths among wavebands.</p> <p><i>FY 2010 Plans:</i>            Next-Generation Core Optical Networks (CORONET)            - Initiate the development of the network control and management software such that the final product will be transitioned and implemented in current commercial and DoD core optical networks.</p> <p>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.</p>				
Intrinsically Assured Mobile Ad-Hoc Networks (IAMANET)*  *Formerly Dynamic Quarantine of Computer-Based Worms (DQW) and Dynamic Quarantine of Computer-Based Worms and Defense Against Cyber Attacks on Mobile Ad-hoc Network Systems (DCAMANET).	7.515	9.432	14.543	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>(U) The Intrinsically Assured Mobile Ad-Hoc Network (IAMANET) program is a continuation of 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).</p> <p>(U) IAMANET will build upon the successes achieved in both the DQW and the DCMANET programs. IAMANET will directly support 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 will be interoperable with fixed networks and may also have potential applicability to the broader DoD network architecture.</p> <p><i>FY 2008 Accomplishments:</i></p> <p>Intrinsically Assured Mobile Ad-Hoc Network (IAMANET)</p> <ul style="list-style-type: none"> <li>- Developed preliminary designs for an assurable network infrastructure (architecture, control and management, algorithms and policies).</li> <li>- Established an independent IAMANET red team to critique the performers during the design of the assurable network infrastructure.</li> </ul> <p>Dynamic Quarantine of Computer-Based Worms (DQW)</p> <ul style="list-style-type: none"> <li>- Integrated DQW system into DoD enterprise networks tool suite.</li> <li>- Integrated DQW prototype into DoD enterprise solution tool suite.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- Tested integrated system against full-spectrum nation state worm threat.</li> </ul> <p><i>FY 2009 Plans:</i> Intrinsically Assured Mobile Ad-Hoc Network (IAMANET)</p> <ul style="list-style-type: none"> <li>- Complete the designs and development of the assurable network infrastructure.</li> <li>- Test and evaluate the performance of the assurable network infrastructure on a 96-node networking simulation.</li> </ul> <p>Dynamic Quarantine of Computer-Based Worms (DQW)</p> <ul style="list-style-type: none"> <li>- Harden system against directed attacks.</li> <li>- Improve detection and response capabilities discovered from testing.</li> <li>- Test integrated system on operational network.</li> <li>- Test integrated system against red teams (attack teams) during Combatant Command exercise.</li> <li>- Transition technology to DoD.</li> </ul> <p><i>FY 2010 Plans:</i> Intrinsically Assured Mobile Ad-Hoc Network (IAMANET)</p> <ul style="list-style-type: none"> <li>- Conduct red team attacks and assessments of the assurable network infrastructure to verify the network's integrity, availability, reliability, confidentiality, and safety.</li> <li>- Initiate the design, development and integration of a secondary defensive subsystem (similar to what was developed under DCAMANET and the Dynamic Quarantine of Worms) with the assurable network infrastructure and a host radio.</li> <li>- Initiate design and development of trusted hardware components for specific key functions.</li> </ul>				
<p>Trustworthy Systems</p> <p>(U) The goal of the Trustworthy Systems program is to provide foundational trustworthy computer platforms for Defense Department computing systems. This program seeks to develop technologies such as novel computer processing architectures, hardware, firmware, or microkernels to guarantee network and workstation security and will initially focus on network-based monitoring approaches that provide maximum coverage of the network with performance independent of the network size. This program will</p>	11.300	9.910	11.090	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>focus on the development of feedback control-based solutions to software vulnerabilities and gateway-and-below network traffic monitoring approaches that scale with network size. Operational goals of the network-monitoring component include: 1) improved probability of detection/probability of false alarm performance and 2) scalability to future gateway line speeds. The desired result is to allow software to be imperfect while mitigating catastrophic failures. Technical challenges include remotely monitoring mission-critical servers using virtual machines, tracking the trustworthiness of the server, and controlling the server to return it to trustworthiness states. Primary end users identified to date include Strategic Command Joint Task Force/Global Network Operations and Headquarters Pacific Command. Transition partners include National Computer Security Center, Naval Information Warfare Activity, and Defense Information Systems Agency.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed scalable formal methods to verify complex hardware/software.</li> <li>- Researched network-sensitive approaches to monitor, and trustworthy controllers to control, how and when information is disseminated across the network based on network performance, load, criticality, and target capacity.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Investigate the use of new virtual machine hardware architectures to develop a feedback loop that enables the host to monitor and control its behavior in the presence of untrustworthy software.</li> <li>- Investigate secure hardware designs, software architectures, and code assessment technologies.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Complete evaluation of client-side controller software in laboratory environment.</li> <li>- Develop client-side laboratory-scale software and server-side virtual-machine based automated recovery.</li> <li>- Harden and evaluate client-side controller code for field-deployable operations.</li> </ul>				
Security-Aware Systems	13.680	10.088	11.225	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>(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).</p> <p>(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 with little or no human assistance. The effort will leverage advances in information assurance research programs to 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.</p> <p>(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</p>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>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.</p> <p>(U) The Scalable Cryptographic Key Management effort seeks to develop a key management and key distribution system with an overall overhead equal to or less than today's key management systems, while servicing thousands--or tens of thousands--of devices. The lack of a scalable key management and distribution system is the fundamental hurdle to the widespread deployment of secure radios and encryption devices to individual desktops. This effort will leverage changes in underlying technology and reduced costs for these new technologies to produce applications that will transition to the Services or via the commercial sector ranging from secure hand-held radios for tactical use to desktop level encryption devices for more secure networks.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed techniques to collaboratively diagnose and respond to problems (e.g., attacks or failures that threaten a mission) in groups of military systems.</li> <li>- Developed techniques to summarize security policy and status so the descriptions produced by the AC program can be understood without omitting critical details.</li> <li>- Developed static and dynamic source code analysis techniques (e.g., data and control-flow-based techniques, model-checking, strong typing) to relate software module structures and runtime state with the representation of security properties/configurations.</li> <li>- Demonstrated self-explanation techniques in which systems explain their critical security properties and status in a manner that is understandable to a variety of managing software components and human operators.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- Developed additional general strategies to automatically immunize systems against new attacks and preempt insider attacks; enabling anomaly detection, combining and correlating information from system layers, and using direct user challenges.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop, test and validate regimes to assess the protection mechanisms of security products, and certify protection to quantifiable levels based on a scientific rationale.</li> <li>- Develop measures to quantitatively characterize various dimensions of security (availability, integrity, confidentiality, authentication, and non-repudiation), fault tolerance, and intrusion tolerance, and demonstrate the theory's relevance by applying it to a realistic exemplar system.</li> <li>- Tailor an exemplar self-regenerative system representative of a military application, thereby demonstrating the protective value to the warfighter.</li> <li>- Conceptualize a new computer workstation architecture that enables both formal proof and exhaustive validation of critical information and program separation properties.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Demonstrate a prototype exemplar self-regenerative system representative of a military application.</li> <li>- Mature, evaluate and transition technologies enabling development of an enterprise network that rapidly identifies, localizes and suppresses attacks and accidental faults automatically, and provides an early warning system that predicts these events.</li> <li>- Develop the architecture to enable a reliable key management system that will issue, revoke, and change the key for 10,000+ users.</li> <li>- Initiate fabrication of affordable key management system components.</li> </ul>				
<p>Control Plane</p> <p>(U) The Control Plane program improved end-to-end network performance between the Continental United States (CONUS) operating base and forward deployed tactical units. Control Plane developed the ability for individual hosts (end-points) to learn essential characteristics about the network, allowing the hosts to shape the network and network traffic to optimize network loading, prioritize traffic, and create communities</p>	5.296	0.000	0.000	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>of interest. Under Control Plane, when multiple network paths are available, hosts are able to choose the best path/community or simultaneously transmit over multiple paths/communities.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed and demonstrated the ability of individual hosts (end-points) to learn essential characteristics about the network path between themselves and their transition partners through network query protocols.</li> <li>- Investigated authentication protocols for secure transmission of network performance information.</li> <li>- Developed and demonstrated the ability of hosts to learn about more than one possible transmission path, other hosts' abilities and purpose, and form communities of interest which suits their collective needs best.</li> <li>- Developed and demonstrated the ability of hosts to simultaneously use multiple network paths for the same data transmission with the same partner, increasing communications speed and reliability.</li> <li>- Conducted demonstrations in operationally relevant environments.</li> </ul>				
<p>Control-Based Mobile Ad-Hoc Networks (CBMANET)</p> <p>(U) The Control-Based Mobile Ad-Hoc Networks (CBMANET) program is developing an adaptive networking capability that dramatically improves performance and reduces life-threatening communication failures in complex communication networks. In order to develop this new capability, the initial focus is on tactical mobile ad-hoc networks (MANETs) that are inadequately supported with commercial technology. Conventional MANETs are composed of interdependent nodes based on interdependent system layers. Each MANET node exposes tens to hundreds of configurable parameters that must be continuously adapted due to variable tactical factors such as mission profile, phase, force structure, enemy activity, and environmental conditions. The complexity of this high-dimensional, adaptive, constrained, distributed network configuration problem is overwhelming to human operators and designers and has root causes in the historically wire-line-oriented networking paradigms. This program will take on the ambitious goal of researching a novel protocol stack that supports integrated optimization and control of all network layers simultaneously. Key technical challenges include scalable design, stability, and convergence. These challenges are particularly difficult in a distributed setting with partial and uncertain information, high communications overhead, and high probability of link failure. To address this problem,</p>	8.060	4.200	0.000	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>the CBMANET program will exploit 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.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Designed appropriate interfaces between the CBMANET network stacks and the physical radios in support of cross-layer optimization.</li> <li>- Integrated the novel network architectures with physical radios and executed field experiments.</li> <li>- Demonstrated and evaluated CBMANET technologies in realistic DoD scenarios using modeling and simulation.</li> <li>- Began conducting a series of field demonstrations in challenging tactical environments, using tactically relevant radios.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Complete development and integration into military radio systems.</li> <li>- Execute final experiments and military demonstrations.</li> <li>- Transition activities to the Services.</li> </ul>				
<p>Code Characterization*</p> <p>*Formerly Defense Autonomous Systems.</p> <p>(U) The Code Characterization program will develop cyber forensic techniques to characterize, analyze and identify malicious code. Today malicious computer code is found through its effects and isolation after infection. Current detection, analysis, and corrective software requires an intensive, manual process that is always conducted afterwards. This program will develop breakthrough abilities in visualization, threat identification analysis and threat mitigation analysis to enable positive identification of malcode sub-structures. By using cross-utilization and cross-domain analysis using these baseline malcode sub-structures, this program will allow for the automatic discovery, identification, and characterization of any future variants of previously unknown malicious code in computing systems.</p>	0.000	3.750	8.500	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Investigate innovative methods of integrating detection techniques to quickly identify malicious code delivered through various file types.</li> <li>- Develop automatic techniques to rapidly and interactively reconstruct (encrypted and non-encrypted) meta data to assist in the analysis of malicious code, or non-white listed software archives.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop techniques and algorithms to enable the characterization of future malicious code variants based on analyzed malware substructures.</li> <li>- Initiate integration of automatic discovery, identification, analysis, and prediction algorithms.</li> <li>- Establish red team to test the malicious code detection techniques.</li> <li>- 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.</li> </ul>				
<p><b>Geo-Steganography</b></p> <p>(U) The Geo-Steganography program will develop techniques for embedding additional information in a wide variety of digital file types in a manner that does not disturb the normal use of the file. This technology will enable tactical end users to add private information to normal digital communication channels, permitting privacy in a multicast, multiuser environment (for example coalition operations). The advantage of steganography is the ability to selectively expose additional private information to only a subset of end recipients within the context of ongoing normal message traffic. This can be accomplished in a way that minimally disturbs the usual file traffic over the channel.</p> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop effective and transparent CONOPS for the use of steganography in operational settings as the basis for technology development and deployment.</li> <li>- Determine the most effective steganography techniques for tactical field use, considering document types, bandwidth impact, and ease of use.</li> </ul>	0.000	0.000	5.000	
DARPA Future Information Assurance Initiatives	2.250	0.000	0.000	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>(U) The DARPA Future Information Assurance Initiatives identified promising technologies to enable remote command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) warfighting. Included in this initiative was the development of secure, efficient network protocols to exploit tomorrow's network-centric technologies such as networked weapons platforms, mobile ad-hoc networks, and end-to-end collaboration (vice client-server paradigm).</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed a family of distributed, autonomous security devices to deal with asymmetric traffic on wide area networks.</li> <li>- Developed a secure, efficient network routing protocol for tomorrow's weapon, logistic, and command and control requirements.</li> <li>- Developed a wireless protocol that securely provides location, authentication, and communications in a practical manner.</li> <li>- Investigated new approaches to network security that scale with increased data rates and address spaces of future networks.</li> </ul>				
<p>Content Distribution</p> <p>(U) This program seeks to provide information to commanders and soldiers before they need it by anticipating their needs. Current systems (e.g., file caches, peer-to-peer networks or Akamai-like systems) watch what users' request and react by either moving data or shifting users to other data stores. These techniques neither move the data beforehand nor work efficiently in bandwidth constrained military environments. The Content Distribution program will combine content retrieval with geographic location aware content "pushing" that predicts what information deployed commanders will need and moves that data from one content network (e.g., in CONUS) to a deployed content retrieval network. The technology developed will provide content to deployed soldiers who are not in command posts by integrating the new content distribution system with the Disruption Tolerant Network (DTN) technology. This will allow the Defense Department to exploit network knowledge and signaling to push information during low network usage periods and reduce overall network loading, providing pre-positioned information so that commanders have the information they need before they need it. This program will also seek to decrease</p>	0.000	0.000	4.750	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>overall data network (e.g., TCP/UDP/IP protocol based networks) loading by accurately predicting the content users will likely request based on past activity.</p> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop a scalable architecture for efficiently publishing metadata on a distributed content network.</li> <li>- Develop network and routing discovery software that pinpoints routing and communications' bottlenecks.</li> <li>- Develop efficient algorithms to encode information to minimize network loading.</li> </ul>				
<p><b>High-Speed Optical Correlator for Next Generation Networks</b></p> <p>(U) The High-Speed Optical Correlator for Next Generation Networks program will investigate key technical areas of a revolutionary, high-speed optical correlator for next generation networks. As the core network data rates of fiber telecommunications increase, existing electronic content processors are challenged in terms of complexity and power consumption. Through the use of a novel optical-based digital pattern matching architecture, and using standard telecommunications components, this program will develop a scalable system that, together with electronic processing, will monitor, secure and assist next generation, very high data rate telecommunication networks (&gt;100 Gbit/s). Successful implementation of this technology will allow existing slower speed, electronic processors to be used for secondary and more complex data processing. This combination of optical and electronic components will allow us to analyze a larger portion of the network traffic than is currently achieved. The useful life of existing electronic processing technology will also be significantly extended, in its role as a post-processor on the pre-sifted data.</p> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop optical-based digital pattern matching architecture and complete the initial design for building the device.</li> <li>- Test critical sub-components to ensure their practicality.</li> <li>- Develop metrics for evaluating hardware components and system effectiveness.</li> <li>- Initiate development of high-speed optical correlator technology.</li> <li>- Complete design for a 1 Gbps prototype.</li> </ul>	0.000	0.000	4.872	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>Millicomputing</p> <p>(U) The Millicomputing program seeks an innovative approach to low-power computing that is anticipated to reduce power consumption by at least fifty percent. Given the increasing quantity of computing devices in military, government, and corporate environments coupled with expensive and uncertain energy resources, there is an urgent need to develop revolutionary technologies that greatly reduce energy use and cost in modern computing systems. The Millicomputing program will drastically reduce power consumption while maintaining high-grade computing performance by matching the computational platform to the user's needs; exploiting concurrency inherent in instruction sets, processes, and applications; and improving resource utilization across the computational platform.</p> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Design and develop computational platform and system design architecture.</li> <li>- Develop millicomputing proof-of-principle testbed.</li> <li>- Initiate develop of prototype system.</li> </ul>	0.000	0.000	4.000	
<p>Trusted, Uncompromised Semiconductor Technology (TrUST)</p> <p>(U) The TrUST program was funded in FY 2008 under PE 0602716E, Project ELT-01. The TrUST program will address in Integrated Circuits (ICs) 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. The follow on effort will seek to discover an understanding of the function of an integrated circuit (IC) which is specified, designed and fabricated by someone untrusted; as is the case when using offshore resources. An example of such an integrated circuit would be a commercial off-the-shelf (COTS) application specific IC (ASIC) or COTS field programmable gate array (FPGA). While the COTS ASIC case is important, the COTS FPGA case is dominant, pervasive, and critical.</p> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- 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<sup>6</sup> transistors in 240 hours.</li> </ul>	0.000	21.186	33.538	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- 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 Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) for a design of 10<sup>6</sup> transistors in 240 hours.</li> <li>- Continue to refine and expand tools for FPGA verification and extend the number of FPGA families that they target for a design of 10<sup>6</sup> transistors in 240 hours.</li> <li>- Protect FPGAs from unauthorized substitutions by improving and empirically verify the software/firmware framework for using Physically Unclonable Functions.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- 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<sup>7</sup> transistors in 120 hours.</li> <li>- 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<sup>7</sup> transistors in 120 hours.</li> <li>- Continue to refine and expand tools for FPGA verification and extend the number of FPGA families that they target for a design of 10<sup>7</sup> transistors in 120 hours.</li> <li>- Protect FPGAs from unauthorized substitutions the program will improve and empirically verify the software/firmware framework for using Physically Unclonable Functions.</li> <li>- Integrate a complete TrUSTed IC solution for ASICs and FPGAs that is ready for transition.</li> <li>- 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.</li> <li>- Identify, develop, and quantify performance of innovative destructive and non-destructive evaluation techniques for 32 nm ICs which can fully evaluate the IC functionality.</li> </ul>				
<p>National Repository of Digital Forensic Intelligence</p> <p>(U) This effort focused on the goal of the National Repository of Digital Forensic Intelligence.</p> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Pursue efforts relating to the National Repository of Digital Forensic Intelligence.</li> </ul>	0.000	1.200	0.000	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009		
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research		<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-03	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>			<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>
Document Analysis and Exploitation <i>FY 2009 Plans:</i> - Conduct research in document analysis and exploitation.			0.000	1.600	0.000
Intelligent Remote Sensing for Urban Warfare <i>FY 2009 Plans:</i> - Conduct research in remote sensing for urban warfare.			0.000	2.400	0.000
<b>C. Other Program Funding Summary (\$ in Millions)</b> N/A					
<b>D. Acquisition Strategy</b> N/A					
<b>E. Performance Metrics</b> Specific programmatic performance metrics are listed above in the program accomplishments and plans section.					

**UNCLASSIFIED**

R-1 Line Item #11

Page 25 of 32

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>								<b>DATE:</b> May 2009		
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research				<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY					<b>PROJECT NUMBER</b> IT-04	
<b>COST (\$ in Millions)</b>	<b>FY 2008 Actual</b>	<b>FY 2009 Estimate</b>	<b>FY 2010 Estimate</b>	<b>FY 2011 Estimate</b>	<b>FY 2012 Estimate</b>	<b>FY 2013 Estimate</b>	<b>FY 2014 Estimate</b>	<b>FY 2015 Estimate</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
IT-04: LANGUAGE TRANSLATION	66.130	75.019	72.171						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)**

	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
Spoken Language Communication and Translation System for Tactical Use (TRANSTAC)	11.064	11.533	7.738	
<p>(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 language tool that will meet the military's language translation needs. TRANSTAC is currently focusing on key languages of the Middle East region.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Performed additional mission needs analysis and aggressive language data collection.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-04	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- Developed new two-way translation software technologies for insertion into, and enhancement of, the two-way Iraqi systems.</li> <li>- Developed tools for rapid deployment of new languages and dialects.</li> <li>- Enhanced recognition and translation performance with a particular emphasis on a military lexicon for Iraqi Arabic.</li> <li>- Developed smaller form-factor prototypes to facilitate mobile use (towards eyes-free, hands-free) translation systems.</li> <li>- Increased robustness of the prototypes to address the issue of noisy environments.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Update/enhance the experimental systems in the field.</li> <li>- Continue mission needs analysis and aggressive language data collection.</li> <li>- Develop two-way translation systems in other languages that will enable the user to not only translate words, but also communicate and carry on limited conversation.</li> <li>- Develop context management translation techniques.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Continue to develop context management translation techniques.</li> <li>- Demonstrate a hands-free, eyes-free two-way translator prototype.</li> <li>- Extend translation techniques to develop translation systems emphasizing other key languages (Dari and Pashto).</li> </ul>				
<p>Global Autonomous Language Exploitation (GALE)</p> <p>(U) The Global Autonomous Language Exploitation (GALE) program will develop and integrate technology to enable automated transcription and translation of foreign speech and text along with content summarization. GALE 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</p>	46.935	46.396	40.015	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-04	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<p>translation accuracy by exploiting context and other clues. GALE will address unstructured speech such as talk show conversations and chat room communications, developing timely, succinct reports and alerts for commanders and warfighters.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Developed methods to optimize the parameters of speech-to-text acoustic models such that transcription errors are minimized.</li> <li>- Developed discriminative training algorithms to optimize word alignment and translation quality.</li> <li>- Implemented an integrated search of speech-to-text transcription and machine translation.</li> <li>- Integrated metadata extraction into the speech-to-text components.</li> <li>- Evaluated translation and distillation technologies.</li> <li>- Incorporated syntactic analysis of the target language (English) with machine translation algorithms to improve translation fluency.</li> <li>- Transitioned preliminary technologies developed by the GALE program into high-impact military systems and intelligence operations centers.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Incorporate syntactic analysis of the source languages (Arabic and Chinese) and develop more accurate word alignments between source and target languages.</li> <li>- Perform 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.</li> <li>- Incorporate predicate-argument analysis to enhance machine translation and summarization.</li> <li>- Develop a new distillation algorithm to extract the 5 W's (who, what, where, when, and why) for given documents and methodologies to evaluate distillation algorithms.</li> <li>- Continue to transition the GALE technologies, as available, into high-impact military systems and intelligence operations centers.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop methods for porting technology into new languages.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-04	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- Complete the architecture for a summarization system that incorporates adaptive filtering, focused summarization, information extraction, contradiction detection, and user modeling.</li> <li>- 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.</li> <li>- Continue to transition technologies developed by the GALE program into high-impact military systems and intelligence operations centers.</li> <li>- Exercise language independent paradigm for new languages essential for military use - Dari, Pashto and Urdu.</li> </ul>				
<p>Multilingual Automatic Document Classification, Analysis and Translation (MADCAT)</p> <p>(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.</p> <p><i>FY 2008 Accomplishments:</i></p> <ul style="list-style-type: none"> <li>- Improved methods for document segmentation (e.g., title, address box, columns, lists, embedded picture/diagram/caption, annotation, signature block, etc.).</li> <li>- Improved script (e.g., Roman vs. Cyrillic) and language (e.g., Farsi vs. Arabic) identification.</li> </ul>	8.131	12.414	16.222	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-04	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
<ul style="list-style-type: none"> <li>- Developed algorithms for document type identification (e.g., letter, ledger, annotated map, newspaper, etc.).</li> <li>- Developed means to discriminate and separate handwriting from printed regions and improved OCR/OHR technologies.</li> <li>- Developed the means of interpreting different regions within a document, such as extracting information from an address field or the axes of a table.</li> </ul> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Develop improved algorithms for document type identification (e.g., letter, ledger, annotated map, newspaper, etc.); to discriminate and separate handwriting from printed regions; and to improve OCR/OHR technologies.</li> <li>- Create better means of interpreting different regions within a document such as extracting information from an address field or the axes of a table.</li> <li>- Develop algorithms to predict the syntactic structure and propositional content of text, and for recognizing and transcribing hand-written text.</li> <li>- 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.</li> <li>- Enable efficient metadata-based search and retrieval.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- Transition tightly integrated technology prototypes to high-impact military systems and intelligence operations centers.</li> </ul>				

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>			<b>DATE:</b> May 2009	
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY		<b>PROJECT NUMBER</b> IT-04	
<b>B. Accomplishments/Planned Program (\$ in Millions)</b>	<b>FY 2008</b>	<b>FY 2009</b>	<b>FY 2010</b>	<b>FY 2011</b>
- Extend language independent technology to languages also using Arabic script - Dari, Pashto and Urdu.				
<p>Robust Automatic Translation of Speech (RATS)</p> <p>(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.</p> <p><i>FY 2009 Plans:</i></p> <ul style="list-style-type: none"> <li>- Improve the robustness of automatic speech transcription and translation algorithms in adverse environments (noise, distortion, reverberation, and competing speech signals).</li> <li>- Evaluate the relative benefits (performance versus computational requirements) of noise suppression and speech exploitation based on a single microphone versus using multi-microphone arrays.</li> <li>- Assess 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, and develop improved methods where required.</li> </ul> <p><i>FY 2010 Plans:</i></p> <ul style="list-style-type: none"> <li>- Continue to improve the robustness of automatic speech transcription and translation algorithms in adverse environments (those with noise, distortion, reverberation, and/or competing speech signals).</li> <li>- Continue to develop noise suppression and speech exploitation based on a single microphone versus using multi-microphone arrays.</li> <li>- Refine new speech processing techniques for noisy environments, including echo suppression, speech activity detection, language identification, speaker identification and keyword spotting.</li> </ul>	0.000	4.676	8.196	

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>Exhibit R-2a, PB 2010 Defense Advanced Research Projects Agency RDT&amp;E Project Justification</b>		<b>DATE:</b> May 2009
<b>APPROPRIATION/BUDGET ACTIVITY</b> 0400 - Research, Development, Test & Evaluation, Defense-Wide/BA 2 - Applied Research	<b>R-1 ITEM NOMENCLATURE</b> PE 0602303E INFORMATION & COMMUNICATIONS TECHNOLOGY	<b>PROJECT NUMBER</b> IT-04
<b>C. Other Program Funding Summary (\$ in Millions)</b> N/A		
<b>D. Acquisition Strategy</b> N/A		
<b>E. Performance Metrics</b> Specific programmatic performance metrics are listed above in the program accomplishments and plans section.		

**UNCLASSIFIED**