RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E

COST (In Millions)	FY 2005	FY2006	FY2007	FY 2008	FY 2009	FY 2010	FY 2011
Total Program Element (PE) Cost	182.815	195.991	242.852	249.651	247.146	245.870	193.870
Intelligent Systems & Software IT-01	12.209	0.000	0.000	0.000	0.000	0.000	0.000
High Performance and Global Scale Systems IT-02	68.909	69.283	82.900	85.000	85.000	85.000	48.000
Information Assurance and Survivability IT-03	48.594	60.964	76.015	79.115	80.977	80.277	65.277
Language Translation IT-04	53.103	65.744	83.937	85.536	81.169	80.593	80.593

(U) <u>Mission Description:</u>

(U) The Computing Systems 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 Intelligent Systems and Software project developed new technology for software creation, processing and database management to significantly improve software for systems that produce, store, and analyze information about battlespace operations. It developed fundamentally new techniques for: (1) transforming signals into descriptions of battlespace entities; (2) exchanging information about entities among different systems at both the syntactic and semantic levels; and (3) managing that information exchange as situations and resources change over time.

(U) The High Performance and Global Scale Systems project develops the computing, networking, and associated software technology base underlying the solutions to computational and information-intensive applications for future defense and federal needs. These technologies will lead to successive generations of more secure, higher performance, and cost-effective systems; associated software technologies; advanced mobile information technology; and prototype experimental applications critical to defense operations.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E

(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 exploit large volumes of speech and text in multiple languages; (b) revolutionize human-computer interaction via spoken and written English and foreign languages; (c) perform computing and decision-making tasks in stressful, time-sensitive situations; and (d) become active, autonomous agents/assistants to analysts, operators and warfighters by collating, filtering, synthesizing and presenting information in timely and relevant forms.

(U) **Program Change Summary:** *(In Millions)*	**FY 2005**	**FY 2006**	**FY 2007**
Previous President's Budget	187.767	198.831	213.723
Current Budget	182.815	195.991	242.852
Total Adjustments	-4.952	-2.840	29.129
Congressional program reductions	-0.146	-2.840	
Congressional increases	0.000		
Reprogrammings	0.000		
SBIR/STTR transfer	-4.806		

(U) **Change Summary Explanation:**

FY 2005 Decrease reflects DOE transfer for P.L. 108-447 and SBIR/STTR transfer.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E

FY 2006	The decrease reflects undistributed reductions for Section 8125 and the 1% reduction for section 3801: Government-wide rescission.
FY 2007	Increase reflects enhancement of the Language Translation project to address technologies to translate documents captured during tactical operations and continue work on two-way tactical speech communications between warfighters and native speakers. The PE increase also addresses funding for Phase III of the High Productivity Computing System (HPCS) program to complete the detailed design, fabrication, integration and demonstration of the first full scale prototypes. New Information Assurance technologies will also be emphasized.

THIS PAGE INTENTIONALLY LEFT BLANK

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)				DATE February 2006			
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research				R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02			
COST (In Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
High Performance and Global Scale Systems IT-02	68.909	69.283	82.900	85.000	85.000	85.000	48.000

(U) Mission Description:

(U) This project develops the computing, networking and associated software technology base required to support future defense and federal needs for computational and information-intensive applications. These technologies will lead to successive generations of more secure, higher performance, and more cost-effective computing systems. The project will also develop critical associated software technologies, advanced mobile information technology, and prototype experimental applications critical to defense operations.

(U) Program Accomplishments/Planned Programs:

	FY 2005	FY 2006	FY 2007
Responsive Computing Architectures	68.909	69.283	82.900

(U) The Responsive Computing Architectures component is bringing much needed flexibility to DoD systems. It is developing integrated computing subsystems that will respond in real time to dramatic changes in mission application requirements and operating constraints based on the mission of the day. Current projects are focused on quality of service, algorithm/application computing diversity and scalable computing efficiency. The technologies being developed here have direct and significant impact for military systems, such as the Land Warrior/Objective Force, ground and airborne autonomous devices, distributed sensors, space sensors and intelligence collection ground systems. The Responsive Computing Architecture component funds the High Productivity Computing Systems program.

(U) The High Productivity Computing Systems (HPCS) program will provide the DoD with significant technology and capability advancements for the national security and industrial communities by filling a critical gap between today’s 1980s-based high performance computing systems and the future promise of quantum computing. This program is targeting high-end, tera-to-petascale computing in medium-to-long-term national security missions where, according to two recent DoD studies, U.S. superiority and security are threatened. The technology development plan is being executed in three phases that will extend to the end of this decade. The three phases are (1) concept study, (2) research

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

and development, and (3) prototype development. HPCS will address a number of critical technology barriers over the next decade including: (1) processor/bandwidth performance efficiency; (2) software availability/reliability for large-scale computing systems; (3) integral hardware, software, application robustness; (4) intrusion resistance; (5) run-time software brittleness; (6) time-to-solution; and (7) cost of developing, operating, maintaining, and upgrading DoD national security applications. Through HPCS technology, performance and efficiency for critical national security applications will realize a forty-fold improvement. Early identification of key mission partner users and their high-end computing application requirements, and development of metrics and performance prediction tools will be used throughout the program to assess accomplishment of both technical milestones and adherence to the schedule.

(U) Program Plans:

- Perform a focused industry R&D Engineering Phase II effort that will evaluate, simulate, and prototype the innovative HPC system architectures selected from the Phase I concept studies.
- Release alpha “value based” productivity metrics and benchmarks to guide future program research and development activities.
- Address large system brittleness by exploring hardware and software reliability and fault tolerance capabilities, active application software bug tolerance, and intrusion identification and resistance.
- Evaluate alternative balanced system architectures comprised of processors, memory, interconnects, software, and programming environments that will result in high productivity computing systems.
- Perform a critical technology assessment and prototype engineering readiness review of the Phase II HPCS petascale systems and their viability for implementation in the 20l0 timeframe.
- Perform a down-select from the Phase II R&D commercial participants based on their readiness for prototype development (Phase III); their ability to address the government’s HPC needs in the 2010-2011 timeframe, and their commercial viability.
- Initiate research prototype development (Phase III) of a high-end petascale computing system with improved time-to-solution characteristics, in collaboration with other government agencies.
- Implement applied high productivity language software and intelligent file system research to support the revitalization of high-end computing.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

(U) <u>Other Program Funding Summary Cost:</u>

- Not Applicable.

THIS PAGE INTENTIONALLY LEFT BLANK

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

COST (In Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Information Assurance and Survivability IT-03	48.594	60.964	76.015	79.115	80.977	80.277	65.277

(U) Mission Description:

(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), the Guidance Technology program element (PE 0603768E), and other programs that satisfy defense requirements for secure, survivable, and network centric systems.

(U) Program Accomplishments/Planned Programs:

	FY 2005	FY 2006	FY 2007
Next Generation Optical Networks	7.521	6.754	6.463

(U) The Next Generation Optical Networks 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) the elimination of data-flow bottlenecks and the enhancement of network scalability through the creation of optical network hardware that minimizes the occurrence of need for optical-to-electrical-to-optical conversions; (2) greatly increased network capacity through the use of more efficient fiber-optical transmission techniques; (3) network management tools that guarantee optimization of high density wavelength-division-multiplexed optical channels, such as those provided by wavelength division multiplexing; (4) creation of a new class of protocols that permit the

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

cross-layer communications needed to support quality-of-service requirements of high-priority national defense applications; and (5) demonstration of novel concepts in intelligent and cognitive switched based networks. This effort will deliver the high-performance inter-networking capabilities needed for development of applications such as distributed and network based command and control, intelligence analysis, predictive logistics management, simulation and scenario enhanced decision-making support for real-time combat operations, and assured operation of critical U.S. networking functions when faced with severe physical layer attack. These network-based functions will support the real-time, fast-reaction operations of senior leadership, major commands and field units.

(U) An important initial component of this program, the Tactical Fiber-Optical Network effort will make it possible for the U.S. military to create a rapidly deployable, self-healing, tactical wavelength-division-multiplexed (WDM) fiber-optical network that can provide substantial communications capability to command centers deployed in somewhat mature areas of hostility. Key capabilities that will be enabled by this program include: (1) the elimination of power needs in the core of the network through the design and fabrication of passive wavelength-routing nodes that will allow the switching functions to be done via tunable optical transmitters and receivers (transceivers) at the edge of the network; (2) enhanced network survivability through a suitable highly connected network topology leveraging a fast-restoration protocol capable of rapid recovery from multiple network node and link failures; and (3) extended geographical coverage of the network to hundreds of kilometers, without requiring additional power at the core. In addition, protocols will be developed to enable the connection of this network to tactical wireless networks as well as to existing fixed legacy networks. The program will also include the development of techniques to realize ruggedized network nodes and interconnecting fiber cables, which are to be buried in the ground or in riverbeds or other waterways.

(U) A companion program, the Millimeter Wave Networks project, explored new technology to make the upper millimeter wave (MMW) region affordable for proliferated use in an operational environment. This project investigated the unique characteristics of the 60GHz band, which attenuates radio signals very rapidly due to absorption, to develop network devices that can transmit the reasonably high levels of power required for high data rates, and still be undetectable at a distance from the network.

(U) Program Plans:

- Next Generation Optical Networks
  - – Create an all-optical hardware design and fabrication to enable regeneration, wavelength switching and sub-wavelength grooming.
  - – Develop and demonstrate an efficient fiber-optical transmission technique to enable several-fold increase in fiber capacity.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Develop switch architecture design and signaling protocols for zero-apparent-jitter, low-latency, real-time applications.
- Develop national testbed hardware specification, local area to wide area network integration, with data-format independence.
- Develop protocols for physical layer-to-application layer connectivity and routing algorithms for optically switched networks.
- Demonstrate the ability to manage frequency and enforce low probability of detection limits.
- Enable the interface between optically switched backbone networks and conventional networks.

- Tactical Fiber-Optical Network
  - Create a suitable architecture for a passive, WDM fiber-optical network with high connectivity for increased reliability.
  - Develop a set of passive, wavelength-routing nodes that can enable the realization of this architecture.
  - Develop a wavelength plan for interconnecting client devices with tunable optical transceivers placed at the edge of the network.
  - Develop a protocol for rapid restoration from multiple network node and link failures through re-tuning the optical transceivers.
  - Conduct an analysis to estimate the resulting network reliability and survivability under various failure scenarios.
  - Demonstrate the ability to interconnect client devices with a wide range of analog and digital signal formats and protocols.
  - Devise appropriate protocols to enable the integration of the network with tactical wireless networks.
  - Develop protocols and interfaces to enable connecting this network to existing legacy networks.
  - Develop techniques to realize ruggedized network nodes and fiber cables.
  - Build and test a network testbed that is representative of a network suitable for one or more target aerospace platforms.

- Millimeter Wave Networks
  - Validated that photonics-based modem and RF sources are orders of magnitude simpler than conventional RF.
  - Determined that the upper millimeter wave region offers increased RF power scaling due to low combining loss which can allow almost unbounded bandwidth.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E, Project IT-03

	FY 2005	FY 2006	FY 2007
Dynamic Quarantine of Computer-Based Worms	14.807	18.643	19.671

(U) The goal of the Dynamic Quarantine of Computer-Based Worms program is to develop defenses for U.S. military networks against large-scale malicious code attacks such as computer-based worms. As the U.S. military pushes forward with network-centric warfare, terrorists and other nation-states are likely to develop and employ malicious code to impede our ability to fight efficiently and effectively. This program will develop the capability to automatically detect and respond to computer-based worm attacks against military networks, provide advanced warning to other DoD enterprise networks, provide rapid recovery of infected systems, study and determine the worm's propagation and provide off-line rapid response forensic analysis of malicious code to identify its capabilities, and future behavior. Additionally, the program will investigate technologies for defense against cyber attacks on mobile ad hoc network (MANET) systems. This effort will develop defenses that can sense failures and attacks on military tactical wireless networks and auto-reconfigure in real-time to provide continuous service of mission-critical activities. This program will develop technology to ensure wireless mobile network centric warfare systems are able to fulfill their mission in spite of runtime hardware/software failures and cyber attacks such as computer worms unleashed on MANETs. This program will develop technology to reconfigure the network, nodes, and platforms for optimal mission execution as a result of changes that may occur in the trustworthiness of the network.

(U) Program Plans:

- Developed and tested automatic detection and quarantine mechanisms.
- Developed and transitioned off-line malicious code analysis capabilities.
- Test auto-quarantine capabilities against more sophisticated threats.
- Develop emulated wireless mobility testbed.
- Develop host and network-based detection and quarantine sensors/actuators for MANET systems.
- Develop application re-provisioning services for failed nodes.
- Verify integrated system capabilities.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E, Project IT-03

	FY 2005	FY 2006	FY 2007
Trustworthy Systems	8.551	9.757	10.058

(U) The goal of the Trustworthy Systems program is to provide foundational trustworthy computer platforms for DoD computing systems. This program seeks to develop technologies such as novel computer processing architectures, hardware, firmware, or microkernels that will guarantee the security and integrity of data processed for secure applications. The military utility of the technology would be to provide high degree of assurance that software systems procured by DoD cannot compromise the DoD missions they support even when compromised by Trojan horse software, or just plain buggy software. Transition targets include weapons platforms, flight control systems, and enterprise software systems. The transition customers are Joint Task Force (JTF)-Global Network Operations and the DoD Enterprise Security Steering Group (ESSG) for providing DoD enterprise wide information assurance solutions.

(U) Initially, an Information Assurance (IA) Transition effort in this project will identify, develop, and transition key information assurance research technologies to DoD networks, filling gaps in commercial off-the-shelf (COTS) tool coverage. Specifically, previously-funded DoD research technologies will be identified, matured, evaluated, and deployed on select DoD networks as a testbed for developmental integration testing. This program provides a framework for advocates of other technologies to be similarly considered for deployment to DoD networks. The desired final output of the program is a more secure DoD network, providing improved protection against current and future threats.

(U) Program Plans:

- Trustworthy Systems
  - Develop hardware, firmware, and microkernel architectures as necessary to provide foundational security for operating systems and applications.
  - Develop tools to find vulnerabilities in complex open source software.
  - Develop scalable formal methods to formally verify complex hardware/software.

- Information Assurance (IA) Transition
  - Mature the technologies to the point they can be operationally tested.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

-- Test and evaluate secure hardware designs, software architectures, and code assessment technologies.
-- Deploy technologies on pilot network.
-- Identify key IA technologies for transition.

	FY 2005	FY 2006	FY 2007
DARPA Future Information Assurance Initiatives	2.009	4.150	5.603

(U) The Department's vision for the future includes comprehensive knowledge of the battlespace and the ability to fight wars with information technology that enables remote C^4ISR operations. Sophisticated computing capabilities like those available in current desktop workstation and server systems are moving to mobile wireless embedded systems that communicate over low bandwidth self-organizing tactical networks often with low-powered devices. Concurrent with the advanced computing capability will be security and other trustworthiness challenges in the systems that the future U.S. military will be heavily dependent upon during battle. With the increased U.S. military dependence on information technology, the ability to maintain battlefield superiority requires control of our information systems against increasingly sophisticated adversaries employing computer network attack. With foreign production of information technology increasing, and adversaries seeking to use the asymmetric leverage of cyber warfare as the Achilles' heel of current and future U.S. military systems; the U.S. military must have the ability to withstand, operate through, and counter increasingly lethal cyber attacks, while reducing the manpower required. The DARPA Future Information Assurance Initiatives will identify promising technologies to continue to push the state of the art and pursue transition opportunities to promote adoption by the military services. Other distinct programs within this project will be created to pursue promising technologies as they are identified for further focused development.

(U) Program Plans:

– Develop automatic techniques to modify computer applications to add information assurance properties e.g. confidentiality, authentication, and others.
– Develop the ability of individual hosts (end-points) to learn essential characteristics about the network path between themselves and their transmission partners.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E, Project IT-03

- Develop the ability to protect the core signaling and control of converged networks running voice over IP (VOIP), wireless, and voice, and data networks in enterprise telecommunications.
- Identify and authenticate hosts on the network with a follow-on goal of allowing these hosts to query the network to discover the network's operating attributes.
- Develop a family of distributed, autonomous firewalls that work together as required to deal with asymmetric traffic on wide area networks.
- Develop a wireless protocol that securely provides location, authentication, and communications in a practical manner.
- Investigate new approaches to network security that scale with increased data rates and address spaces of future networks.

	FY 2005	FY 2006	FY 2007
Control Plane	3.597	5.752	7.956

(U) The Control Plane Program will improve end-to-end network performance between the Continental United States (CONUS) operating base and forward deployed tactical units. Control Plane seeks to develop the ability for individual hosts (end-points) to learn essential characteristics about the network, allowing the hosts to shape the network in a way that optimizes network loading, prioritizes traffic, and creates communities of interest among nodes in large networks. Additionally, when multiple network paths are available, hosts will be able to choose the best path/community or simultaneously transmit over multiple paths/communities. This technology will support the Defense Department's Global Information Grid concept of operations.

(U) Program Plans:

- Develop mechanisms to improve end-to-end wide-area network performance between the Continental United States (CONUS) operating base and forward deployed tactical units.
- Develop the ability of individual hosts (end-points) to learn essential characteristics about the network path between themselves and their transmission partners through network query protocols.
- Investigate authentication protocols for secure transmission of network performance information.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E, Project IT-03

– Develop 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.
– Develop the ability of hosts to simultaneously use multiple network paths for the same data transmission with the same partner, increasing communications speed and reliability.

	FY 2005	FY 2006	FY 2007
Wide Area Network (WAN) Monitoring	1.267	2.408	4.300

(U) The Wide Area Network (WAN) Monitoring effort seeks to develop distributed network monitoring capabilities and devices that can be used to identify, characterize, enable, optimize and protect the WANs that compose the Global Information Grid (GIG). This program will develop advanced capabilities to monitor the WANs that will comprise the GIG in to detect information flows that are indicative of malicious behavior, routing problems, or compromised mission capability. Goals include improved detection and false-alarm performance over conventional intrusion detection systems and scalability to the larger networks. This technology will support the Department of Defense's Global Information Grid Information Assurance technical framework.

(U) Program Plans:

– Develop algorithms representing that quickly characterize various host's security configurations, identity, and classification as well as measure the type and quantity of information exchange.
– Develop high-throughput hardware to implement the algorithms at the sensor layer.
– Develop low-latency networks to collect the information.
– Develop high-speed analyzers to assimilate the data and detect perturbations.
– Integrate and test components in a fully functional configuration.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	**DATE** February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	**R-1 ITEM NOMENCLATURE** Information and Communications Technology PE 0602303E, Project IT-03

	FY 2005	FY 2006	FY 2007
Spread Spectrum Networking	0.000	0.000	2.900

(U) Spread spectrum communication technology will significantly improve security against a variety of network attacks and identification profiles by spreading energy over a broad bandwidth, thereby providing an adversary with a signal which is both difficult to detect, as well as difficult to jam without using significant resources. This program expands these same goals, by addressing not just the physical layer but also the entire network stack. Similar to frequency-hopping spread spectrum, the approach of this program is to develop and demonstrate algorithms that provide hopping between IP addresses and then expanding to hopping between different permutations of layer 1-3 protocols. The utility is to provide significantly improved security against a variety of network attack and identification profiles.

(U) Program Plans:

– Determine the most effective cross layer spreading techniques through analysis and simulation.
– Implement these techniques on relevant platforms.
– Demonstrate the effectiveness of these techniques against network attack.

	FY 2005	FY 2006	FY 2007
Control-Based Mobile Ad-Hoc Networks	0.000	4.500	6.099

(U) An outgrowth of the Trustworthy Systems and the DARPA Future Information Assurance Initiatives, the Control-Based Mobile Ad-Hoc Networks (CBMANET) program will develop 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). MANETs are composed of interdependent nodes based on interdependent system layers. Each 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 wireline-oriented networking

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

paradigms. Today's commercial trends are not aimed at supporting the DoD's extreme deployments or unique applications. 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, 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 and situation awareness.

(U) Program Plans:

- Design and develop a novel protocol architecture from first principles in information theory and optimization theory.
- Design and demonstrate protocols based on network coding that vastly improve performance in extreme conditions.
- Design and demonstrate cross-layer protocols and adaptive control capabilities to drive resource allocation more efficiently.
- Design novel control interfaces to support DOD-relevant applications such as multicast and situation awareness.
- Design appropriate interfaces between the novel network stack and the physical radio platforms to support cross-layer optimization.
- Perform quantitative analysis and trade studies to understand the degree of performance offered by the novel network stack.

	FY 2005	FY 2006	FY 2007
Security-Aware Systems	6.103	9.000	12.965

(U) Today's military software systems are brittle in the face of changing requirements. They are vulnerable to skilled attackers who develop creative and unpredictable strategies, and are increasingly dependent on software produced in and/or "outsourced" to potentially hostile nations. Misconfiguration accounts for most security failures in internet services and poses a serious risk to military 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

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)		DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03	

techniques augmented with cognitive decision-making techniques with the ultimate goal of applying these systems on to the Global Information Grid.

(U) This Security-Aware Systems thrust was previously budgeted in the DARPA PE 0602304E, Project COG-01. It has been enhanced with technologies and approaches developed under the Trustworthy Systems, Asymmetric Flow Monitoring and the DARPA Future Information Assurance Initiatives, programs within this project. The Security-Aware Systems thrust will also explore practical advanced software engineering technology for building flexible systems that will allow new features to be added via “interposition” between existing features, with guaranteed levels of reliability and security. Cognitive and automated software analysis techniques will screen outsourced software both for quality lapses and unauthorized functionality to assure the outsourced code performs as expected. Strategies for intelligently adapting complex system configurations in response to operator action will be developed. Cognitive reconfiguration technology will infer the user’s legitimate goals and adapt configurations to rapidly meet those goals with a minimal impact on security and longer-term objectives. The Security-Aware Systems thrust encompasses the Application Communities (AC) program together with several supporting research initiatives.

(U) The Application Communities (AC) program will leverage the research conducted under DARPA’s information assurance programs to create a new generation of self-defending software that automatically responds to threats, and provide a comprehensive picture of security properties and current status 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, thus increasing the speed and confidence with which military systems can be securely and dynamically reconfigured, particularly under stressful conditions. 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 stealth attacks (where attackers take control of systems undetected).

(U) Research initiatives related to vulnerabilities, missions and threats in computer abstract-model reasoning will enable systems to create a prioritized list of threats and analyze the hypotheses about threats in the context of system development and deployment. The resulting technology will enable current systems to generate vulnerability reports ranked by probable impact of a failure/attack on the mission. In addition, technology that results in a multi-level network operating system capable of controlling the flow of classified information will prevent unauthorized leakage through computer systems, and provide planners and intelligence analysts safe, simultaneous, and convenient access to classified and unclassified information.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

(U) Program Plans:

- Develop techniques to collaboratively diagnose and respond to problems (e.g., attacks or failures that threaten a mission) in groups of military systems.
- Demonstrate automated techniques for reasoning about and understanding the security-relevant interactions between software components of military systems.
- Develop techniques to summarize security policy and status so the descriptions produced by AC can be understood without omitting critical details.
- Augment current techniques to construct a framework for developing high-assurance behavioral specifications (including security policies). Formulate a unified knowledge base to represent the properties and capabilities of disparate security mechanisms.
- Develop 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.
- Demonstrate 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.
- Develop test and validation regimes to assess the protection mechanisms of security products and certify protection to quantifiable levels based on a scientific rationale.
- 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.
- Develop techniques for practical construction of extensible software and analysis techniques for predicting the effects of new functionality inserted into a system.
- Develop a theory of code to formalize the properties of interposition and stimulate a new wave of software reliability and productivity improvement.
- Demonstrate cognitive security analysis of complex multi-component software systems.
- Develop an ontology of system and security configuration settings and ontology-based techniques that infer and express operator goals.
- Build information flow tracking and dynamically-reconfigurable event interposition into modeling techniques and their supporting tools.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Develop reasoning techniques to evaluate the impact of negative scenarios on a system design and anticipated mission scenarios.
- Develop network switches that provably control information flows according to a specified policy.
- Develop ubiquitous, intelligent software agents that learn and respond to attacks on Global Information Grid infrastructure scale.
- Integrate developed technologies into the Global Information Grid.

	FY 2005	FY 2006	FY 2007
Fault Tolerant Networks	1.000	0.000	0.000

(U) The primary goal of the Fault Tolerant Networks program has been to develop technologies that provide for continuous and correct network operation even when attacks are successful. By developing reliable, ad-hoc, and adaptive networking protocols that allow for communications between peers during conditions of known or suspected faults or attacks in wide-area networks, this program has developed technologies to dramatically improve communications across the network. This program was designed to seek a number of different networking protocols and technologies to improve network security and provide quantitative statistical metrics that allow for the objective evaluation of network performance when fault condition exists or attacks are on-going or suspected.

(U) Program Plans:

- Developed a unified model for multi-path communication.
- Developed protocols for reliably communicating between peers in ad-hoc networks and adaptive multi-path forwarding protocols for tolerating and adapting to faults in wide-area networks.
- Demonstrated attack profiling and filtering algorithms that discard a high percentage of Distributed Denial of Service (DDoS) traffic and a low percentage of non-DDoS traffic.
- Extended an overlay network prototype to integrate boundary security, enforcing overlay separation and preventing leakage of traffic onto the base network.
- Demonstrated statistical measures that are both efficient and effective at detecting traffic that contributes to a DDoS attack that originates multiple network “hops” back from the attack target.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Implemented and evaluated distributed queuing in prototype router hardware while continuing fundamental studies of distributed queuing algorithms, with a focus on algorithms that support reservation-oriented traffic.
- Developed tools for measuring and communicating the structure of network topologies in both wide-area and mobile environments and for measuring underlying latencies, service times, and characteristics that constrain the best possible network availability solutions.

	FY 2005	FY 2006	FY 2007
Dynamic Coalitions	1.000	0.000	0.000

(U) The Dynamic Coalitions program has developed technologies that allow the formation of partnerships between and across organizations that are seeking joint collaboration to provide secure networking communications, improve policy management and group communications, and provide for the improved security of infrastructure services and data sharing. Given that future U.S. military operations will be increasingly “joint,” involving multiple branches of the U.S. Armed Forces and, potentially allied or other coalition forces, secure and accessible communication will be critical for future war-fighting scenarios outlined in Joint Vision 2020. This effort has leveraged recent advancements in wireless networking technologies by investigating those technologies that can migrate coalition information assurance tools from servers to gateway radios, thereby allowing such functionality to spread throughout the coalition. The most promising technologies sought under this program are being tested in operationally relevant experiments with U.S. warfighters in DARPA’s Partners in Experimentation program which is also budgeted in this project.

(U) Program Plans:

- Developed a new formalism for application level policies to accommodate new aspects of policy that do not manifest at the network layer, such as access control mechanisms.
- Developed specific technology to enable multi-level network management and multi-level message passing.
- Completed the implementation of the surrogate trust negotiation architecture for supporting trust negotiation in a wireless environment.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Experimentally proved that architectures that incorporate reusable tickets or tokens can eliminate the need for repetitive, heavyweight trust negotiations between protected resources within a security domain without compromising the security of the overall system.
- Demonstrated adaptors to a policy engine for a set of real networking, monitoring and control technologies including: network management tools; commercial firewalls; and application specific entities such as web servers.

	FY 2005	FY 2006	FY 2007
Partners in Experimentation	2.739	0.000	0.000

(U) The Partners in Experimentation program conducted security technology experimentation with operational military and coalition partners. As part of this effort, the program developed relationships with partners that led to multi-application information sharing, as well as improving interoperability between the participating partners. Such experimentation also led to the development of technologies for distributed denial of service countermeasures and encryption techniques to secure email across multiple organizations working collaboratively. Operational experimentation provided valuable feedback to the security technology research and development process; demonstrated the benefits of advanced technology; and accelerated technology transition.

(U) Program Plans:

- Transitioned Identity Based Encryption to the United States Northern Command (USNORTHCOM) for communicating sensitive but unclassified data between Department of Defense and local, state and other Federal non-DoD agencies as well as non-governmental agencies.
- Demonstrated identity-based encryption techniques to secure email in a multi-organization collaborative environment.
- Demonstrated secure group communication capability for informal trust relationships.
- Provided the capability for cross-domain information sharing for an interoperability demonstration.
- Constructed and demonstrated a trusted patch management system as well as an Information Assurance Vulnerability Assessment (IAVA) compliance checking capability.
- Evaluated performance and scalability of lab-proven anomaly detection techniques for intrusion detection in real-world, high-volume environments.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)		DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03	

- Demonstrated network monitoring and Distributed Denial of Service (DDoS) countermeasures.
- Demonstrated multi-application cross-domain information sharing capability.

(U) **Other Program Funding Summary Cost:**

- Not Applicable.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)							DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research				R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04			
COST (In Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Language Translation IT-04	53.103	65.744	83.937	85.536	81.169	80.593	80.593

(U) Mission Description:

(U) This project will develop and test powerful new technology for processing human languages that will provide critical capabilities for a wide range of national security needs. This technology will enable systems to (a) automatically exploit large volumes of speech and text in multiple languages; (b) revolutionize human-computer interaction via spoken and written English and foreign languages; (c) perform computing and decision-making tasks in stressful, time-sensitive situations; and (d) autonomously collate, filter, synthesize and present relevant information in timely and relevant forms.

(U) Program Accomplishments/Planned Programs:

	FY 2005	FY 2006	FY 2007
Situation Presentation and Interaction	10.900	16.373	20.837

(U) The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program will develop 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 will build on existing speech translation platforms developed in the previous Compact Aids for Speech Translation program to create a rapidly deployable language tool that will meet the military's language translation needs. For example, the program will add a two-way translation capability and will include Arabic dialects spoken in Iraq (the current Phraselator uses only Modern Standard Arabic).

(U) Program plans:

- Perform mission needs analysis and aggressive initial language data collection.
- Develop and evaluate a two-way spoken English-Iraqi Arabic communication device for Stability and Support Operations and tactical missions.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

- Demonstrate an initial two-way Iraqi system.
- Develop new two-way translation software technologies for insertion into and enhancement of the two-way Iraqi systems.
- Develop techniques for the system to learn and adapt in the field.
- Perform continuous in-field language data collection.

	FY 2005	FY 2006	FY 2007
Automated Speech and Text Exploitation in Multiple Languages	42.203	49.371	63.100

(U) This thrust includes the Global Autonomous Language Exploitation (GALE) program which leverages technologies developed under two predecessor programs: Translingual Information Detection, Extraction and Summarization (TIDES), a program that developed new capabilities for translation (converting foreign language material to English), detection (finding or discovering needed information, e.g. topics), extraction (pulling out key information including entities and relations), and summarization (substantially shortening what a user must read); and Effective, Affordable, Reusable Speech-To-Text (EARS), a program that created transcription (speech-to-text) technology for broadcasts, telephone conversations and multiparty speech that were either stand alone products or inputs to TIDES technologies.

- Global Autonomous Language Exploitation (GALE) will revolutionize the exploitation of both speech and text in multiple languages (which is currently slow, labor-intensive, and limited) by developing core enabling technologies and end-to-end systems for insertion into a series of high-impact military and intelligence operational settings. GALE will substantially improve upon and exploit capabilities developed under TIDES, build upon the successes of both TIDES and EARS, and emphasize the creation of a systems framework for integrating the component language processing technologies, evaluating them based on their utility in various end-user tasks. GALE technology will enable machines to convert and distill enormous volumes of streaming speech and text in many languages to provide critical intelligence. Specifically, the GALE technologies will provide an English translation of foreign speech and text into English text with extremely high accuracy (95%). GALE technologies will also distill text from both the English sources and the output of the translation engines to pinpoint the concise portions of documents that are relevant to military users, eliminating the need to browse through huge volumes of information. This program will research speech processing technology that has the potential to address spoken utterances in hostile, noisy environments.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

- A follow-on program, Multilingual Automatic Document Classification, Analysis and Translation (MADCAT), will address the recurring military problem of understanding the content of documents captured during tactical operations. These documents often contain machine printed and handwritten text in various combinations and orientations in one or more languages. MADCAT devices would enable soldiers to convert these documents to readable English in the field. Such documents contain perishable information and timely translation is critical. Currently, the military does not have the resources to meet this critical demand. The MADCAT program will substantially improve document analysis and OCR/OHR (optical character recognition/optical handwriting recognition) technology, integrate it tightly with translation technology, and assemble technology demonstration prototypes for field trials.

(U) Program Plans:

- Transition technologies developed by TIDES and EARS into high-impact military systems and intelligence operational centers including CENTCOM, SOCOM and MARFORPAC.
- Develop methods for porting TIDES technology to new languages.
- Leverage TIDES and EARS research to develop technology to convert huge volumes of streaming speech and text in multiple languages into English text by transcribing English speech while simultaneously transcribing and translating foreign speech and text.
- Develop technology to distill critical intelligence from English text by improving information retrieval, extraction and information tracking techniques.
- Design and document an architecture based on the Unstructured Information Management Architecture (UIMA) that was extended and enhanced for GALE.
- Identify workflows of all processing engines and provide integration of these workflows on top of the architectural foundation.
- Architecturally support the creation of components that combine the output of multiple machine translation engines.
- Develop an integrated approach where the problem is viewed mathematically as a single system, with foreign speech/text as input and English text and distilled information as output.
- Develop methods to optimize the parameters of speech-to-text acoustic models such that transcription errors are minimized on the training data.
- Implement an integrated search of speech-to-text transcription and machine translation.
- Develop discriminative training algorithms to optimize word alignment and translation quality.
- Develop technology to enable processing of speech uttered in hostile, noisy environments.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-04

- – Develop technology for robust speech recognition with noise suppression and multi-input and output blind source separation.
- – Develop algorithms to predict the syntactic structure and propositional content of text.
- – Develop technology to convert captured documents into readable and searchable English.
- – Improve and exploit document segmentation, language and type identification, and script and ideographic character recognition technology.
- – Insert GALE technologies and systems into high-impact military and intelligence operations centers.

(U) <u>Other Program Funding Summary Cost:</u>

- Not Applicable.