RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)						DATE February 2005		
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research			R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, R-1 # 12					
COST (In Millions)	FY 2004	FY 2005	FY 006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total Program Element (PE) Cost	0.000	187.767	198.831	213.723	245.838	245.670	235.670	230.670
Intelligent Systems & Software IT-01	0.000	16.550	0.000	0.000	0.000	0.000	0.000	0.000
High Performance and Global Scale Systems IT-02	0.000	60.130	70.143	75.000	100.000	100.000	100.000	100.000
Information Assurance and Survivability IT-03	0.000	53.698	62.944	69.036	70.617	70.077	70.077	70.077
Language Translation IT-04	0.000	57.389	65.744	69.687	75.221	75.593	65.593	60.593

(U) Mission Description:

(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. This program element and the four projects included within it were created in accordance with congressional intent in the FY 2005 DoD appropriations bill with prior year funding budgeted in PE 0602301E, Projects ST-11, ST-19, ST-24, and ST-29.

(U) The Intelligent Systems and Software project develops 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 develops 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 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, R-1 # 12

(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**	**FY2006**	**FY2007**
Previous President's Budget	191.456	226.016	248.989
Current Budget	187.767	198.831	213.723
Total Adjustments	-3.689	-27.185	-35.266

Please note that this program element has been newly created from projects previously funded in PE 0602301E. The *Previous President's Budget* amount reflects projects ST-11, ST-19, ST-24, and ST-29 funded under that PE.

Congressional program reductions	-4.889
Congressional increases	1.200
Reprogrammings	0.000
SBIR/STTR transfer	0.000

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, R-1 # 12

(U) Summary Explanation:

FY 2005	Decrease reflects congressional undistributed reductions offset by a congressional add for Secure Group Communications.
FY 2006 – 2007	Decrease reflects the termination of Project IT-01 in FY 2006 as programs transfer to the Network Centric Enabling Technology project (TT-13) in PE 0602702E. This decrease is offset by an increase in the Language Translation project (IT-04) where the next generations of speech and text translation devices are budgeted.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)							DATE February 2005	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research			R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-01					
COST (In Millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Intelligent Systems and Software IT-01	0.000	16.550	0.000	0.000	0.000	0.000	0.000	0.000

(U) Mission Description:

(U) This project develops new technology for software creation, processing, and database management to significantly improve software for systems that produce, store, and analyze information about battlespace operations. The software generates 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 information exchange as situations and resources modify over time. First, the design of complex Command, Control, Communications and Computation Intelligence, Surveillance, and Reconnaissance (C^4ISR) systems are accelerated by formalizing descriptions of semantics, performance, and resource levels and developing design tools to use those formalisms to assemble systems. Second, the software enables field integration of legacy systems by providing general purpose tools that use these formalisms to search, browse, display, and combine services available to a command center, especially in coalition environments. This program element and project were created in accordance with congressional intent in the FY 2005 DoD appropriations bill. Prior year funding was budgeted in PE 0602301E, Project ST-11 and is noted as a memo entry in each program below.

(U) Program Accomplishments/Planned Programs:

	FY 2004	FY 2005	FY 2006	FY 2007
DARPA Agent Markup Language (DAML)	(8.916)	10.545	0.000	0.000

(U) The DARPA Agent Markup Language (DAML) program will develop military software tools for use on Intelink and other emerging Command and Control Link systems. The focus of the program is to develop technologies that enhance interoperability and extend the reach of the World Wide Web to programs, sensors, and other data sources. Moreover, the program will enable agent-based programs to share information through those mechanisms. DAML will develop a software language linking the information of a web resource to machine-readable semantics (ontology) which describes both data contents and service providers. This effort will provide new technologies for the intelligent integration of information across a wide variety of heterogeneous military sources and systems in real time. In addition, DAML is developing and evaluating a

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-01

set of tools to transform existing intelligence and command/control software and enables the operation in network-centric computing environments, through the use of DAML ontologies and service descriptions. Without these automated tools, the cost of bringing older software systems into network-centric computing environments can be prohibitive. DAML tools help correlate application-specific ontologies to shared database schema, construct translators from application data structures to database schema, and build mediators that convert product streams from publishers to subscribers.

(U) Program Plans:

- Perform experimental analysis on and deploy Intelink DAML Briefing and Search Tools on an operational Intelink node.
- Demonstrate and prototype DAML tools for web applications for the Military and National Intelligence Community.
- Prototype suite of additional tools to encapsulate legacy software to support DAML ontologies, logics, and service descriptions.
- Conduct experimental analysis of DAML applications.
- Build example mediators to convert data among DAML ontologies, referencing external knowledge bases.

	FY 2004	FY 2005	FY 2006	FY 2007
Automatic Target Recognition Technology	(4.502)	5.000	0.000	0.000

(U) The Automatic Target Recognition Technology (ATRT) program will develop new sensor exploitation aids to detect targets in high volume sensor data with minimal human support. This program will support very large sets of targets (thousands of target types) with high identification performance and very low false alarm rates, as well as develop modeling methods to account for target variability, caused by partial damage, design difference, or equipment loaded onto the exterior of the vehicle. The program will support interaction with humans to supply operational context, guide hypothesis development, and adapt models. By developing techniques for in-the-field training of models, signatures, and scoring parameters, ATRT will identify vehicle-specific signatures and develop new target fingerprinting techniques. Finally, new methods to assist humans in achieving precise identification of ad hoc, poorly defined targets will be developed. The program supports rapid and accurate detection, recognition, and identification of targets in high volume sensor imagery. The imagery will enable a dramatic reduction in sensor-to-shooter timelines, supporting dynamic target engagement. Follow-on efforts are being pursued in PE 0603767E, Project SEN-02.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-01

(U) Program Plans:
- Obtain a regular supply of data from field and developmental sensors, covering numerous target types in many environmental settings.
- Estimate ground truth for those data to provide a foundation for periodic performance assessments.
- Extend existing performance analyses to provide bounds on detection, identification, and fingerprinting performance for thousands of vehicle types.
- Develop model generation, model update, detection, recognition, identification, and fingerprinting algorithms based on a range of technical approaches.
- Periodically assess technologies on the field data, computing statistically significant estimates of performance to compare against the analyses.

	FY 2004	FY 2005	FY 2006	FY 2007
Rapid Software Composition for Embedded Systems	(2.477)	1.005	0.000	0.000

(U) The Rapid Software Composition for Embedded Systems program develops technology to permit rapid assembly of heterogeneous C^4ISR components for execution on complex, highly parallel, real-time embedded architectures. The technology will explore techniques to permit rapid parallel code development and optimization and to leverage advanced architectures for development, exploration, and rapid deployment of C^4ISR components. This program will provide tools and software libraries that allow C^4ISR systems to be rapidly assembled from discrete, pretested components. In addition, developers will be assisted in assembling and tailoring C^4ISR systems for mission-specific tasks. Furthermore, the technology will facilitate mapping C^4ISR system components onto advanced run-time architectures for high performance operations in limited footprint environments (airborne, tactical vehicle, afloat). The tools created will optimize new C^4ISR capabilities using spiral development processes without loss of performance.

(U) Program Plans:
- Identify a set of challenge applications across the spectrum of C^4ISR missions.
- Assemble a library of kernel algorithm components.
- Map the kernel components onto representative hardware architectures.
- Develop input/output/state descriptions of each kernel component, as mapped to each architecture.
- Construct tools to assemble kernel components into systems, including data flows and process/processor assignments.
- Build predictive models of systems assembled from kernel components.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-01

- Verify run-time feasibility and achievement of required performance.
- Validate the tools and models within the challenge applications.

(U) Other Program Funding Summary Cost:

- Not Applicable.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
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 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
High Performance and Global Scale Systems IT-02	0.000	60.130	70.143	75.000	100.000	100.000	100.000	100.000

(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. The project comprises two primary components – Responsive Computing Architectures and Network Embedded Technology. This program element and project were created in accordance with congressional intent in the FY 2005 DoD appropriations bill. Prior year funding was budgeted in PE 0602301E, Project ST-19 and is noted as a memo entry in each program below.

(U) Program Accomplishments/Planned Programs:

	FY 2004	FY 2005	FY 2006	FY 2007
Responsive Computing Architectures	(78.351)	60.130	70.143	75.000

(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 energy/power management, quality of service, algorithm/application computing diversity and scalable computing efficiency. The technologies 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 comprises Power Aware Computing and Communications, and High Productivity Computing Systems.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

(U) The Power Aware Computing and Communications (PAC/C) program is developing an integrated software and hardware power management technology suite comprising novel techniques that may be applied to all levels of a system from the chip/device level to the algorithm/application level. Embedded military computing systems such as future Land Warrior systems, autonomous devices, distributed sensors and space sensors have demanding dynamic computational requirements, but extremely limited energy resources. PAC/C will enable embedded computing systems to reduce energy requirements by ten to one hundred times for energy-constrained military applications ranging from hand-held computing devices to unmanned aerial vehicles.

(U) The High Productivity Computing Systems (HPCS) program will provide DoD with significant technology and capability advancements for the national security and industrial communities by filling a critical gap between today's late 1980's 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 and development, and (3) full-scale development. HPCS will address a number of critical technology barriers over the next decade: (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 high-end computing application requirements, metrics and performance prediction tools will be used throughout the program to assess both technical and schedule progress.

(U) Program Plans:

- Power Aware Computing and Communications.
  - -- Provided a beta release of the PAC/C energy-aware simulator and modeling framework for the PAC/C subscale developers to evaluate.
  - -- Develop the final subscale demonstration projects.
  - -- Execute the final PAC/C demonstrations.

- High Productivity Computing Systems.
  - -- 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.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

-- 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 comprising of processors, memory, interconnects, software, and programming environments that will result in high productivity computing systems.
-- Perform critical technology assessment and full-scale engineering readiness review of the Phase II HPCS petascale systems and their viability for implementation in the 20l0 timeframe.
-- Perform down-select from the Phase II R&D participants based on their readiness for full scale development (Phase III), their ability to address the government's HPC needs in the 2010-2011 timeframe, and their commercial viability.
-- Implement basic and applied software research in the revitalization of high-end computing.

	FY 2004	FY 2005	FY 2006	FY 2007
Network Embedded Technology	(20.010)	0.000	0.000	0.000

(U) The Network Embedded Technology component developed software technology for distributed, real-time, and embedded applications, ranging from tens of computing nodes to over a million. Each program is driven by carefully selected Open Experimental Platforms to facilitate the continuous evaluation of progress and end-user influence. By using major theoretical breakthroughs during the past decade in hybrid systems, statistical physics, finite-size scaling, generative programming, and distributed control, the programs have a solid foundation to achieve the ultimate goal of revolutionizing how software-intensive embedded platforms are built for the DoD.

(U) The program has developed technology to support faster and more reliable development of tactical software – that is, distributed real-time and embedded software for tactical applications, and in particular for the time-critical targeting domain. This technology is enabling programmers to safely and productively integrate so-called "cross-cutting" aspects, such as concurrency, synchronization, security, and memory management, with core functionality that implements the interaction of tactical software with the diverse and evolving suite of sensors and actuators that constitute the sensor-to-decision maker-to-shooter chain. The reusable code-base, tools and reference applications delivered by the program more effectively exploit human effort to produce high-quality software that has the adaptability, robustness, and efficiency required by time-critical targeting systems.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-02

(U) Program Plans:

-- Developed scalable techniques for validation of tactical embedded software by computerized analysis of models of the system.
-- Developed language representation and compilation techniques for fine-grained and coarse-grained; aspect-oriented programming of tactical embedded systems.
-- Developed a mechanism whereby quality-controlling functionality can be packaged in a portable and reusable form, and that is suitable for automated integration by the analysis and composition tools.
-- Developed model-driven tools and representations for generating military system software that supports *flexible binding*, meaning that the allocation of resources to software functions may take place at any time after system design, up to and including during deployed system operation.
-- Developed quality-of-service enabled services for persistence, fault tolerance, and high-bandwidth sensor data transmission, such as those services that are required by the highly dynamic nature of modern air-to-ground warfare.
-- Developed catalogs of patterns and pattern languages that formalize the successful techniques associated with developing tactical embedded systems middleware and applications.

(U) Other Program Funding Summary Cost:

- Not Applicable.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
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 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Information Assurance and Survivability IT-03	0.000	53.698	62.944	69.036	70.617	70.077	70.077	70.077

(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 by the Command and Control Information Systems (Project CCC-01, PE 0603760E), Information Integration Systems (Project CCC-02, PE 0603760E), Joint Warfare System (Project NET-01, PE 0603764E), Maritime Systems (NET-02, PE 0603764E), and other programs that satisfy defense requirements for secure, survivable, and network centric systems. This program element and project were created in accordance with congressional intent in the FY 2005 DoD appropriations bill. Prior year funding was budgeted in PE 0602301E, Project ST-24 and is noted as a memo entry in each program below.

(U) Program Accomplishments/Planned Programs:

	FY 2004	FY 2005	FY 2006	FY 2007
Fault Tolerant Networks	(2.191)	2.000	0.000	0.000

(U) The primary goal of the Fault Tolerant Networks program is 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. The program also seeks a number of different networking protocols and technologies that will improve network security and provide quantitative statistical metrics that allow for the objective evaluation of network performance when

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

fault condition exists or attacks are on-going or suspected. These technologies are reducing the amount of damage sustained during an attack, allowing networks to maintain an acceptable, minimum level of functionality. Technologies for strengthening networks have been developed by introducing fault tolerance capabilities against possible attacks at the network level, emphasizing integrity and availability. In addition, technologies for mitigating potential vulnerabilities associated with denial of service attacks have been developed. The most promising of these technologies 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 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.
- Implement and evaluate distributed queuing in prototype router hardware while continuing fundamental studies of distributed queuing algorithms, with a focus on algorithms that support reservation-oriented traffic.
- Develop 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.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2004	FY 2005	FY 2006	FY 2007
Dynamic Coalitions	(2.009)	2.000	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.
- Experimentally prove 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.
- Demonstrate 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.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2004	FY 2005	FY 2006	FY 2007
Partners in Experimentation	(2.544)	5.843	0.000	0.000

(U) The Partners in Experimentation program seeks to conduct security technology experimentation with operational military and coalition partners. As part of this effort, the program also seeks to develop relationships with partners that will lead to multi-application information sharing, as well as improving interoperability between the participating partners. Such experimentation may also lead to the development of technologies for distributed denial of service countermeasures and encryption techniques to secure email across multiple organizations working collaboratively. Operational experimentation will also seek to provide valuable feedback to the security technology research and development process, which will demonstrate to operational personnel the benefits of advanced technology, and accelerate 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.
- Evaluate performance and scalability of lab-proven anomaly detection techniques for intrusion detection in real-world, high-volume environments.
- Demonstrate network monitoring and Distributed Denial of Service (DDoS) countermeasures.
- Demonstrate multi-application cross-domain information sharing capability.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

	FY 2004	FY 2005	FY 2006	FY 2007
Next Generation Optical Networks	(5.556)	7.521	5.754	6.023

(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: the elimination of data flow bottlenecks through the creation of optical network hardware that minimizes the occurrence of optical-to-electrical-to-optical conversions, network management tools that guarantee optimization of high density optical channels such as those provided by wavelength division multiplexing, the 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 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) A companion program, the Millimeter Wave Networks project, is developing new technology to make the upper millimeter wave (MMW) region affordable for proliferated use in an operational environment. This project is leveraging 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 with regeneration capability and optical wavelength switching.
  - -- Conduct network data flow/bottleneck analysis, 10 Gb/s to end user.
  - -- Develop switch architecture design for zero-apparent-jitter real-time applications.
  - -- Develop national testbed hardware specification, local area to wide area network integration, with data-format independence.
  - -- Protocol development for physical layer-to-application layer connectivity.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

-- Demonstrate the ability to manage frequency and enforce low probability of detection limits.
-- Enable the interface between optically switched backbone networks and conventional networks.
-- Provide routing services for optically switched networks.

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

	FY 2004	FY 2005	FY 2006	FY 2007
Dynamic Quarantine of Computer-Based Worms (was Dynamic Quarantine of Worms)	(10.438)	14.807	18.643	17.321

(U) The goal of the Dynamic Quarantine of Computer-Based Worms (formerly known as Dynamic Quarantine of Worms) 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 epidemiology, and provide off-line rapid response forensic analysis of malicious code to identify its capabilities, modalities, 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.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
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 automatic detection and quarantine mechanisms.
- Provide real-time and off-line analysis capabilities.
- Develop emulated wireless mobility testbed.
- Develop host and network-based detection and quarantine sensors/actuators.
- Develop application re-provisioning services for failed nodes.
- Verify integrated system capabilities.

	FY 2004	FY 2005	FY 2006	FY 2007
Trustworthy Systems	(6.854)	9.996	12.534	14.523

(U) The goal of the Trustworthy Systems program is to provide foundational trustworthy computer platforms for tactical military applications. 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. This includes the ability to process multiple classification levels with insecure data and programs on the same platform.

(U) The exemplar system being developed under this program is a handheld wireless personal digital assistant for network centric applications that would permit concurrent operation of situational awareness and command & control applications with unclassified and untrusted Internet/NIPRNET applications. The device could take classified data feeds of multiple classification levels, provide guaranteed separation, authorized cross-domain transactions with assurance of no cross-contamination (e.g., Unclassified – Secret and vice versa), and restrict data to the level that only the user is authorized to see. Innovations from this effort would eliminate traditional red-black separation architectures and short-circuit the long, arduous but fallible certification procedure for multi-level security systems. Additionally, this program will provide the U.S. Armed Forces with better network encryption devices that enable future coalition and joint force organizations to conduct network operations over multiple security domains without sacrificing network efficiency/speed.

(U) The traditional focus for encryption device development is high-speed encryption devices that can be installed on the backbone of the network. Unfortunately, these are expensive, coarse grained, difficult to configure and key, do not support access controls, and cannot be released

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

to most of our allies. The Edge Encryptor effort will provide low-cost encryptors with fine-grained controls—a paradigm shift with respect to our current encryption methods. In addition, these devices will enable better interoperability and data exchange between partners. Efforts to devise and implement improved policy changes will be pursued that will allow these improved encryption devices to be used to encrypt U.S. classified traffic as long as that traffic remains on a U.S. installation.

(U) Finally, the Secure Group Communications effort will develop the mathematical models required for successful evaluation of secure communicating systems. It will focus on the dual aspects of design and analysis of authentication protocols.

(U) Program Plans:

- Trustworthy Systems.
  - -- Develop hardware, firmware, and microkernel architectures as necessary to provide guaranteed separation of data as necessary.
  - -- Develop assured cross-domain sharing of information.
  - -- Develop proofs of separation.
  - -- Engineer device with notional applications.
  - -- Conduct Red Team assessments and demonstrate the technology's utility.

- Edge Encryptors.
  - -- Design and certify improved encryption devices that are able to work with current and projected network equipment and anticipated technologies and be releasable to coalition partners.
  - -- Demonstrate the ability to support wire keying/re-keying.
  - -- Develop certification and transition plans for these improved encryption devices.

	FY 2004	FY 2005	FY 2006	FY 2007
DARPA Future Information Assurance Initiatives	(0.000)	4.569	4.135	5.025

(U) DARPA has been at the forefront of advancing the state of the art for information assurance technologies. Many of today's commercial practices have their roots in previous DARPA investments. As the DoD continues to be reliant upon commercial networks it is paramount that DARPA continue to look forward and investigate promising technologies. The 21st century transformation of the U.S. military will be more

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

dependent on information technology for C^{4}ISR and combat functions than perhaps any other aspect of the military. To a large extent, future combat systems will be more dependent on information than armor to accomplish missions successfully. The Department's vision for the future includes near-perfect knowledge of the battlespace and the ability to fight wars with information technology that enables remote C^{4}ISR 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 to do so. 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, non-repudiation, and others.
- Develop the ability of individual hosts (end-points) to learn essential characteristics about the network path between themselves and their transmission partners.
- Develop an operating system with higher assurance, higher performance, and higher functionality than current A1 systems.
- Develop computing languages, compilers, and systems capable of producing executable code verified to be correct and bug free.
- Protection of Signaling Networks: Develop the ability to protect the core signaling and control of converged networks running voice over IP (VOIP), 3G wireless, and voice, and data networks in the backbone telecommunications switching fabric.
- Identify hosts securely and authoritatively 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 small, lightweight encryption device that is usable for coalition SECRET and below information that is low cost, self-configuring, and releasable to coalition partners.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

- Develop a wireless protocol that securely provides location, authentication, and communications in a practical manner.

	FY 2004	FY 2005	FY 2006	FY 2007
Control Plane	(3.005)	3.597	5.752	7.569

(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 path between themselves and other hosts, allowing the hosts to shape any transmission to pass through the network with the minimal network load. Additionally, when multiple network paths are available, a host will be able to either choose the path that best meets its requirements or simultaneously transmit over multiple paths. This technology will support the Defense Department's Global Information Grid concept of operations.

(U) Program Plans:

- Develop mechanisms to improve end-to-end Transmission Control Protocol and Internet Protocol (TCP/IP) 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.
- Develop the ability of hosts to learn about more than one possible path, choose the one which suits their needs best, and use it.
- Develop the ability of a host to simultaneously use multiple network paths for the same data transmission with the same partner, increasing communications speed and reliability.

	FY 2004	FY 2005	FY 2006	FY 2007
Wide Area Network (WAN) Monitoring (formerly Asymmetric Firewalls)	(0.000)	3.365	6.178	6.369

(U) The WAN Monitoring effort seeks to develop distributed network monitoring devices that can be used to identify traffic flows over the WAN. To do this, the system must deal with asymmetric flows and act to overcome these skewed flows with negligible impact on the network.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

The envisioned technologies include hardware devices for high-speed communications links and software-based changes for slower links. These devices and supporting software code will correctly monitor symmetric flows while simultaneously coordinating with similar devices embedded elsewhere in the network to monitor asymmetric flows. The technology to monitor WAN traffic at the packet, flow, session and application does not currently exist. Being able to monitor and stop unwanted traffic on the WAN and network backbones will dramatically improve network defense.

(U) Program Plans:

- Collect data to enable management and analysis of flows, session, and applications.
- Collect data that enables management and analysis of individual workstations and enclaves within Defense Department networks.
- Develop protocols, devices, and software that will analyze traffic at the packet, session, and application layer level.
- Develop high-speed distributed cueing systems to identify symmetric and asymmetric flow conditions/locations and that will stop unwanted connections across wide area networks before these connections are completed.
- Develop software that aids in the detection/mitigation of asymmetric flows.
- Develop high-speed hardware devices that aid in the detection/mitigation of asymmetric flows throughout the network.

	FY 2004	FY 2005	FY 2006	FY 2007
Code and Network Vulnerability Testing Methodologies	(0.000)	0.000	4.325	4.956

(U) The goal of the Code and Network Vulnerability Testing Methodologies program is to establish an institute to research network phenomena by providing tools, techniques, and methodologies for testing networked computer systems for vulnerabilities. Such an institute is envisioned as a key asset to relevant DoD/U.S. Government agencies whose charter includes seeking to ensure access to information systems, maintaining the U.S. edge in information operations, leveraging advances in information technologies, and ensuring DoD's ability to provide end-to-end interoperable communications in the long-term. The institute would develop the techniques and formal methods to validate the 'networthiness' of networked weapons systems. Currently, software/firmware/hardware systems can be checked for correct behavior and code security at the individual program or module level. However, once these systems are integrated into a network, they are assumed to work correctly across the network. Generally, there is no effort to validate this assumption and there are no established procedures or methodologies to validate these systems. As a result, the Defense Department's reliance on networks for future operations may be jeopardized.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
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:
- Working with likely DoD transition partners, such as the Defense Information Systems Agency (DISA) or the Directorate of Test and Evaluation (DOT&E), establish goals, evaluation criteria and metrics needed to thoroughly vet potential research institutes.
- Finalize transition plans and agreements with transition partner(s) and obtain approval from USD, Acquisition, Technology and Logistics.
- Select and establish a research institute at a university or non-profit organization that best meets all desired criteria.
- Complete transition to DoD partner as the institute gains operational functionality.

	FY 2004	FY 2005	FY 2006	FY 2007
Remote Direct Memory Access (RDMA)	(0.000)	0.000	5.623	7.250

(U) The Remote Direct Memory Access (RDMA) Protocol Termination Engine (PTE) project is a new and efficient way to develop hardware and software technology that removes the end-system protocol termination bottleneck that limits system access network bandwidth and degrades quality of service delivered to applications. This effort will develop hardware and software to implement these functions on a network interface card rather than in the host processor as is currently the case. The hardware is an ASIC chip implemented in Complementary Metal Oxide Semiconductor (CMOS) that protocol terminates open-standard 10GbE and supports remote direct memory access (RDMA). The software is device driver software that supports the hardware and minimizes loading the system host. The RDMA PTE (RPTE) technology that will be developed enables a wide range of new interoperable open-standards based applications for high performance military systems that use 10 Gb/s broadband networks.

(U) Program Plans:
- Complete design and documentation of the micro-architecture and software specification for the RPTE interface card.
- Complete design and documentation of the PTE implemented in the Field Programmable Gate Arrays (FPGA).
- Simulate RPTE performance in a wide range of applications and compare the results to a conventional approach.
- Fabricate RPTE chips and cards.
- Demonstrate RPTE system.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Information and Communications Technology PE 0602303E, Project IT-03

(U) Other Program Funding Summary Cost:

- Not Applicable.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)							DATE February 2005	
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 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Language Translation IT-04	0.000	57.389	65.744	69.687	75.221	75.593	65.593	60.593

(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. This program element and project were created in accordance with congressional intent in the FY 2005 DoD appropriations bill. Prior year funding was budgeted in PE 0602301E, Project ST-29, and is noted as a memo entry in each program below.

(U) Program Accomplishments/Planned Programs:

	FY 2004	FY 2005	FY 2006	FY 2007
Situation Presentation and Interaction	(10.870)	11.500	11.616	14.387

(U) There are two programs involving direct speech-to-speech translation:

- The Compact Aids for Speech Translation (CAST) program is providing the tactical warfighter with real-time, face-to-face speech translation during combat and humanitarian operations in foreign territories. The program addresses domain-specific translation accuracy and response time. Early CAST prototypes relied on simple dictionaries and phrases. The CAST program resulted primarily in quickly making one-way translation systems (from English to multiple foreign languages) available to warfighters in the field. The DARPA Phraselator is the key prototype system in use today. The system was deployed in Operation Iraqi Freedom and Operation Enduring Freedom. Future versions will offer a more sophisticated, flexible and fluid translation and paraphrasing capability that is robust and conducive to normal human conversations.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Computing Systems and Communications Technology PE 0602303E, Project IT-04

- 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 CAST 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:

– Compact Aids for Speech Translation.
  -- Integrated speech recognition engines into natural language parsers and translators.
  -- Produced prototype translation devices in three languages (Pashto, Farsi, and Mandarin Chinese).
  -- Performed initial coordination with U.S. Army PM Soldier for software integration into land warrior Block III (version 3.0).
  -- Populated the language digital resource repository at Defense Language Institute.

– TRANSTAC.
  -- 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.
  -- Demonstrate 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 ongoing in-field language data collection.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Computing Systems and Communications Technology PE 0602303E, Project IT-04

	FY 2004	FY 2005	FY 2006	FY 2007
Automated Speech and Text Exploitation in Multiple Languages	(43.542)	45.889	54.128	55.300

(U) There are three programs involving the exploitation of naturally occurring speech and text:

- Translingual Information Detection, Extraction and Summarization (TIDES) is revolutionizing the way time-critical intelligence is obtained from speech and text. The program has been developing technology to enable English-speaking operators and analysts to exploit the huge amounts of foreign speech and text (broadcast and newswire) that currently go unanalyzed due to shortages of skilled foreign language analysts. TIDES is creating 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). TIDES technology will dramatically increase the quantity, quality, and timeliness of analysis and reporting, thereby providing vital information to senior decision-makers and enabling commanders to carry out critical missions more swiftly, safely, and effectively.

- Effective, Affordable, Reusable Speech-To-Text (EARS) is creating new automatic transcription (speech-to-text) technology whose output is substantially richer and more accurate than previously possible. Fast, accurate, automatic transcription of broadcasts, telephone conversations and multiparty speech will make rapid search and analysis of speech possible. EARS also provides text versions of spoken language for input to systems developed in TIDES, thereby extending the scope of what is possible with automatic translation, detection, extraction, and summarization.

- 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 off of 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. Captured documents will be converted into readable, searchable English text.

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)	DATE February 2005
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA2 Applied Research	R-1 ITEM NOMENCLATURE Computing Systems and Communications Technology PE 0602303E, Project IT-04

(U) Program Plans:

– Translingual Information Detection, Extraction and Summarization (TIDES).
  -- Demonstrated the ability to detect and track events described in English, Arabic and Chinese news sources.
  -- Demonstrated the ability to extract information from English, Arabic and Chinese news sources.
  -- Demonstrated the ability to translate Arabic newswire text into readable English.
  -- Transitioned successful components to CENTCOM.
  -- Developed methods for porting TIDES technology to new languages.

– Effective Affordable Reusable Speech-To-Text (EARS).
  -- Substantially improved the speed and accuracy of automatic transcription for broadcasts and conversations in English.
  -- Improve the speed of automatic transcription to real time.
  -- Develop automatic techniques to produce rich, readable transcripts of broadcasts and telephone conversations in English, Chinese, and Arabic.
  -- Develop automatic techniques to produce rich, readable, searchable transcripts of multiparty speech from command centers, teleconferences and meetings.
  – Create and evaluate technology demonstration prototypes.

– Global Autonomous Language Exploitation (GALE).
  -- Develop technology to convert huge volumes of streaming speech and text in multiple languages to English text.
  -- Develop technology to distill critical intelligence from that English text.
  -- Develop technology to convert captured documents into readable and searchable English.
  -- Insert these technologies and systems into high-impact military and intelligence operational centers.

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

- Not Applicable.