| | |
|---|---|
| **Exhibit R-2**, **RDT&E Budget Item Justification:** PB 2016 Defense Advanced Research Projects Agency | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400: *Research, Development, Test & Evaluation, Defense-Wide* **/** BA 2: *Applied Research* | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* |

| COST ($ in Millions) | Prior Years | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total | FY 2017 | FY 2018 | FY 2019 | FY 2020 | Cost To Complete | Total Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total Program Element | - | 370.643 | 324.407 | 356.358 | - | 356.358 | 364.076 | 355.357 | 368.535 | 368.091 | - | - |
| IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* | - | 66.481 | 29.800 | 51.490 | - | 51.490 | 58.659 | 58.379 | 63.846 | 58.413 | - | - |
| IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY* | - | 172.063 | 179.947 | 208.957 | - | 208.957 | 240.177 | 245.501 | 249.833 | 254.923 | - | - |
| IT-04: *LANGUAGE TECHNOLOGY* | - | 74.332 | 45.511 | 60.897 | - | 60.897 | 65.240 | 51.477 | 54.856 | 54.755 | - | - |
| IT-05: *CYBER TECHNOLOGY* | - | 57.767 | 69.149 | 35.014 | - | 35.014 | - | - | - | - | - | - |

## A. Mission Description and Budget Item Justification

The Information and Communications Technology program element is budgeted in the applied research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies.

The High Productivity, High-Performance Responsive Architectures project is developing the necessary computing hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include supercomputer, embedded computing systems, and novel design tools for manufacturing of defense systems.

The Information Assurance and Survivability project is developing the core computing and networking technologies required to protect DoD's information, information infrastructure, and mission-critical information systems. The technologies will provide cost-effective security and survivability solutions that enable DoD information systems to operate correctly and continuously even under attack.

The Language Technology project will develop human language technologies to provide critical capabilities for a wide range of national security needs ranging from knowledge management to low-resource language understanding. This project develops technologies to automatically translate, collate, filter, synthesize, summarize, and present relevant information in timely and relevant forms. The Language Technology project is addressing these diverse requirements by developing core language processing technologies and integrating these technologies into operational prototypes suitable for use in the field.

The Cyber Technology project develops technology to increase the security of military information systems and the effectiveness of cyber operations. Over the past decade the DoD has embraced net-centric warfare by integrating people, platforms, weapons, sensors, and decision aids. Adversaries seek to limit this force multiplier

| | |
|---|---|
| **Exhibit R-2**, **RDT&E Budget Item Justification:** PB 2016 Defense Advanced Research Projects Agency | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research* | **R-1 Program Element (Number/Name)**<br>PE 0602303E *I INFORMATION & COMMUNICATIONS TECHNOLOGY* |

through cyber attacks intended to degrade, disrupt, or deny military computing, communications, and networking systems. Technologies developed under the Cyber Technology project will ensure DoD net-centric capabilities survive adversary cyber attacks and will enable new cyber-warfighting capabilities.

| **B. Program Change Summary ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016 Base** | **FY 2016 OCO** | **FY 2016 Total** |
|---|---|---|---|---|---|
| Previous President's Budget | 399.597 | 334.407 | 339.844 | - | 339.844 |
| Current President's Budget | 370.643 | 324.407 | 356.358 | - | 356.358 |
| Total Adjustments | -28.954 | -10.000 | 16.514 | - | 16.514 |
| • Congressional General Reductions | - | - | | | |
| • Congressional Directed Reductions | - | -10.000 | | | |
| • Congressional Rescissions | - | - | | | |
| • Congressional Adds | - | - | | | |
| • Congressional Directed Transfers | - | - | | | |
| • Reprogrammings | -17.142 | - | | | |
| • SBIR/STTR Transfer | -11.812 | - | | | |
| • TotalOtherAdjustments | - | - | 16.514 | - | 16.514 |

**Change Summary Explanation**

FY 2014: Decrease reflects below threshold and omnibus reprogrammings and the SBIR/STTR transfer.

FY 2015: Decrease reflects congressional reduction.

FY 2016: Increase reflects initiation of new start programs in the High-Productivity, High-Performance Responsive Architectures project and expansion of the Low Resource Languages for Emergent Incidents (LORELEI) Technology effort.

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

| COST ($ in Millions) | Prior Years | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total | FY 2017 | FY 2018 | FY 2019 | FY 2020 | Cost To Complete | Total Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* | - | 66.481 | 29.800 | 51.490 | - | 51.490 | 58.659 | 58.379 | 63.846 | 58.413 | - | - |

## A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computer hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems. One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build large complex software systems. Powerful new approaches and tools are needed to enable the rapid and efficient production of new software, including software that can be easily changed to address new requirements and can adjust dynamically to platform and environmental perturbations. The project will ensure accessibility and usability to a wide range of application developers, not just computational science experts.

| B. Accomplishments/Planned Programs ($ in Millions) | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| ***Title:*** Power Efficiency Revolution For Embedded Computing Technologies (PERFECT)<br>***Description:*** The Power Efficiency Revolution For Embedded Computing Technologies (PERFECT) program will provide the technologies and techniques to overcome the power efficiency barriers which currently constrain embedded computing systems capabilities and limit the potential of future embedded systems. The warfighting problem this program will solve is the inability to process future real time data streams within real-world embedded system power constraints. This is a challenge for embedded applications, from Intelligence, Surveillance and Reconnaissance (ISR) systems on unmanned air vehicles through combat and control systems on submarines. The PERFECT program will overcome processing power efficiency limitations by developing approaches including near threshold voltage operation, massive and heterogeneous processing concurrency, new architecture concepts, and hardware and software approaches to address system resiliency, combined with software approaches to effectively utilize resulting system concurrency and data placement to provide the required embedded system processing power efficiency.<br>***FY 2014 Accomplishments:***<br>- Developed an analytical modeling framework for fundamental design trade-off analysis and documentation for local resilience and power optimizations and global optimization methodologies and techniques. Included delivery of initial IBM layered analytical framework addressing concept specification of cross-layer resiliency optimization methodologies, power performance/optimal voltage selection, and throughput performance that developed fundamental trade-off capabilities for power, performance, and | 41.253 | 23.800 | 23.800 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|

reliability for a given embedded system and application space. Included release of improved generation of UC Berkeley Chisel 2.0 hardware construction language for design exploration and generation.
- Established algorithmic analysis and design methodologies for power efficient and resilient processing. Included first practical implementation of communication-avoiding rectangular matrix multiplication using a communication-optimal recursive algorithm, outperforming the Intel Math Kernel Library hand-optimized implementation by up to 10x.
- Defined power efficient, heterogeneous, highly concurrent conceptual architectural design approaches. Test and verification team evaluation report of results to date confirmed collective capabilities to obtain program goal of 75 GFLOPS/W embedded system performance. The evaluation was based on design concepts for power efficient architecture implementations.
- Defined and evaluated the impact of 3D approaches for power efficient processing, including design and simulation of a 3D-stacked Logic-in-Memory (LiM) system architecture to accelerate the processing of sparse matrix data. Simulation results outperform state-of-the-art server and GPU systems by 100x in performance and 1000x in energy efficiency.

***FY 2015 Plans:***
- Incorporate test chip results - circuit, architecture, communication, power management, 3D - for design optimization and simulation refinement for continuing architectural development efforts.
- Develop compiler algorithms supporting communication-avoiding optimization, concepts for optimizing parallel codes and language-based auto-tuning.
- Deliver system-level integrated analytical modeling methodology and software analysis toolset for cross-layer, energy-constrained resilience optimization, processor, memory, and energy-reliability trade-offs.
- Publically release new hardware description language and modeling/simulation infrastructure incorporating the evaluation and development of algorithms, specializers, hardware architectures, and resiliency techniques.

***FY 2016 Plans:***
- Identify and select implementation and transition targets and establish collective PERFECT teams technologies to support target requirements.
- Extend device models to include different physical device scattering mechanisms including acoustic phonon scattering and the impact of quantum mechanical effects on device level characteristics and provide updated device models and libraries of logic gates and memory bit cells incorporating optimization methodologies for super threshold and near threshold operation.
- Complete hardware design evaluations for: low voltage on-chip RAM; adaptive clocking; low-energy signaling; energy-efficient architecture hierarchies; application-specific processing; specialized DRAM architectures; diverse heterogeneous architectures.
- Develop the language constructs and compiler technology supporting the implementation of communication avoiding algorithms and the optimizing and managing of processor heterogeneity, concurrency, data locality, and language based autotuning.
- Implement modeling and evaluation environment integration combining separate optimization tools for power, communication avoidance, and resiliency to provide detailed trade-off analysis results and insight and demonstrate on a range of (1) ISR

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | | **Date:** February 2015 |
|---|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* | |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| kernels (2) PERFECT hardware targets, and (3) problem instance sizes to support 20X power savings incorporating resiliency requirements relative to classical compilers on representative PERFECT hardware architectures. | | | |
| ***Title:*** Complexity Management Hardware* | - | 6.000 | 12.190 |
| ***Description:*** *Formerly Cortical Processor<br><br>The battlefield of the future will have more data generators and sensors to provide information required for successful combat operations. With networked sensors, the variety and complexity of the information streams will be even further extended. In this project, we will develop silicon designs which help alleviate the complexity inherent in next generation systems. These systems will have increasingly large data sets generated by their own multidomain sensors (such as RF and Electro-Optical/Infrared (EO/IR) payloads) as well as potentially new inputs from external sensors. With current programming approaches, there are laborious coding requirements needed to accommodate new data streams. Additionally, the context provided by these data sets is ever changing, and it is imperative for the integrated electronics to adapt to new information without a prolonged programming cycle. Providing contextual cues for processing of data streams will alleviate the fusion challenges that are currently faced, and which stress networked battlefield systems. As opposed to the intuition and future-proofing that is required at the programming stage of a current system, the silicon circuit of the future will be able to use contextual cues to adapt accordingly to new information as it is provided.<br><br>The applied research aspects of this program will look at the circuit design which can exploit the algorithms showing benefit for complexity management. This will entail various sparse versus dense data manipulations with hardware implementations catered to both types of data. The program will show hardware implementations that gracefully handle multiple data streams and limit the programming burden for a complex scenario. Basic research for the program is budgeted in PE 0601101E, Project CCS-02.<br><br>***FY 2015 Plans:***<br>- Design complexity management processor algorithm and benchmark tests for object recognition in still images and action recognition in video.<br>- Demonstrate critical features of algorithm including ability to learn and adapt while operating.<br>- Quantify impact of using low precision, sparse network connectivity on accuracy of results.<br>***FY 2016 Plans:***<br>- Design transistor level circuits implementing the complexity management algorithms.<br>- Demonstrate the ability to manage multiple data streams with interlaced information. | | | |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Create initial hardware verification of concepts for both sparse and hardware demonstrations. | | | |
| ***Title:*** Scalable Optical Nodes for Networked Edge Traversal (SONNET)<br>***Description:*** Graph analytics on large data sets is currently performed on leadership-class supercomputers that are designed for other purposes. These machines are required because they have the memory capacity required for large graph problems, but the demand on the processors is low, resulting in extremely low compute efficiency. Computationally, graph analysis is characterized by many short, random accesses to memory which is inefficient on current systems that are optimized for regular, predictable access. The SONNET program will build a silicon photonics-based graph processor that will perform graph analysis on Terabytes (TBs) of data with performance comparable to peta-scale supercomputers in a significantly smaller size, weight, and power (SWAP) envelope. SONNET will optimize the design of the graph processor by co-designing processor and photonic hardware, and the computer and network architectures to exploit the high bandwidth provided by silicon photonics. SONNET will demonstrate a scalable, power efficient prototype of such a graph processor and quantify performance for DoD-relevant applications. The performance, efficiency, and size will be transformational for big data analytics and enable real-time analysis on dynamic graphs in the fields of cyber security, threat detection, and numerous others. This program will explore the efficient processing of local information using stacked memory and integrated circuits specially made for specific tasks, as well as the efficient transfer of data between local information processors.<br>The SONNET program will optimize the design of a graph processor and design and demonstrate high performance processor cores to accelerate graph primitives and photonic hardware required for high bandwidth, low diameter photonic networks. The program will design and evaluate a Graph processor capable of analyzing large data sets relevant to future DoD requirements. This program has advanced technology development efforts funded in PE 0603760E, CCC-02.<br>***FY 2016 Plans:***<br>- Identify common graph primitives that would accelerate the execution of DoD-specific applications.<br>- Explore the applications benefitting from the unique architecture and whether unique hardware design allows for processors for unique military applications.<br>- Design corresponding hardware, e.g. processor cores, to optimize performance for high bandwidth photonic networks.<br>- Design algorithms to execute DoD problems on a SONNET system and estimate system performance. | - | - | 3.500 |
| ***Title:*** Electronic Globalization<br>***Description:*** Approximately 66% of all installed semiconductor wafer capacity is in Asia. This creates a significant risk for the DoD as off-shore manufacturing of microelectronic components could introduce various vulnerabilities to DoD systems that utilize these non-U.S. fabricated electronic components. As the DoD is faced with this globalization reality, it is essential to prevent | - | - | 12.000 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| potential consequences such as reverse engineering, theft of U.S. intellectual property, and non-authorized use of these electronic components in adversary defense systems.<br><br>New applied research technology enablement will be developed in the Electronics Globalization program to provide the desired responses such as special chip packaging, on-board infrastructures, process modifications, and the use of Supply Chain Hardware Intercepts for Electronics Defense (SHIELD)-monitor dielet. Applied research will focus on the engineering of unique devices and circuit technologies. Concepts and design flows which enable trust in an untrusted environment will be developed and applied. Basic research for the program is budgeted in PE 0601101E, Project ES-01.<br><br>***FY 2016 Plans:***<br>- Develop a specific CONOP using the proposed structure, and identifying key enablers needed to realize it.<br>- Model designs such as encryption engines used to enable authorized chip operation.<br>- Create and model process module modifications for a standard fab gate recipe that result in desired behaviors.<br>- Demonstrate proof-of-concept of the ability of SHIELD-like devices to selectively authorize chip operation.<br>- Complete a high level design of piggyback chips which can monitor and alter instruction execution of the host component. | | | |
| ***Title:*** Instant Foundry Adaptive Through Bits (iFAB)<br><br>***Description:*** Instant Foundry Adaptive Through Bits (iFAB), provided the groundwork for the development of a foundry-style manufacturing capability--taking as input a verified system design--capable of rapid reconfiguration to accommodate a wide range of design variability and specifically targeted at the fabrication of military ground vehicles. The iFAB vision was to move away from wrapping a capital-intensive manufacturing facility around a single defense product, and toward the creation of a flexible, programmable, potentially distributed production capability able to accommodate a wide range of systems and system variants with extremely rapid reconfiguration timescales. The specific goals of the iFAB program were to rapidly design and configure manufacturing capabilities to support the fabrication of a wide array of infantry fighting vehicle models and variants.<br><br>Once a given design was developed and verified, iFAB took the formal design representation and automatically configured a digitally-programmable manufacturing facility, including the selection of participating manufacturing facilities and equipment, the sequencing of the product flow and production steps, and the generation of computer-numerically-controlled (CNC) machine instruction sets as well as human instructions and training modules. iFAB was mostly an information architecture. Only the final assembly capability needed to be co-located under a single roof in anything resembling a conventional fabrication facility; the rest of iFAB could be geographically distributed and can extend across corporate and industrial boundaries, united only by a common model architecture and certain rules of behavior and business practices. The final assembly node of the iFAB Foundry was the Joint Manufacturing and Technology Center (JMTC) at the Rock Island Arsenal (RIA). | 9.734 | - | - |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 / *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| ***FY 2014 Accomplishments:***<br>- Completed the manufacture and assembly of the winning drivetrain and mobility subsystem design from the first FANG Challenge.<br>- Provided manufacturability feedback to the META design process in support of the tool validation testing.<br>- Transitioned iFAB software tool suite and associated technology to the Digital Manufacturing and Design Innovation Institute (DMDII) through the co-funded research and formal technology transition activities for industry use.<br>- Transitioned all physical infrastructure for the iFAB Foundry final assembly node at RIA to JMTC. | | | |
| ***Title:*** META<br>***Description:*** The goal of the META program was to develop novel design flows, tools, and processes to enable a significant improvement in the ability to design complex defense systems that could be verified by virtual testing. The program sought to develop a design representation from which system designs can quickly be assembled and their correctness verified with a high degree of certainty. Such a "fab-less" design approach was complemented by a foundry-style manufacturing capability, consisting of a factory capable of rapid reconfiguration between a large number of products and product variants through bitstream re-programmability, with minimal or no resultant learning curve effects. Together, the fab-less design and foundry-style manufacturing capability was anticipated to yield substantial---by a factor of five ---compression in the time to develop and field complex defense and aerospace systems.<br>***FY 2014 Accomplishments:***<br>- Concluded expanded development of META tool suite to include qualitative and relational abstraction modeling, probabilistic certificate of correctness calculations, complexity metric evaluation, non-linear Partial Differential Equation (PDE) analysis, and cyber design evaluation.<br>- Conducted preliminary developmental Beta testing and integrated demonstration testing for the expanded META tool suite including expanded capability features.<br>- Conducted META tool transition activity to commercial Product Lifecycle Management (PLM) tool suites.<br>- Transitioned META software tool suite and associated technology to the Digital Manufacturing and Design Innovation Institute (DMDII) through the use of co-funded research and formal technology transition activities for industry use.<br>- Further expanded META Software tool suite accessibility by developing a web-based solution for the Generic Modeling Environment (GME). | 15.494 | - | - |
| **Accomplishments/Planned Programs Subtotals** | 66.481 | 29.800 | 51.490 |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-02 **/** *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES* |

## C. Other Program Funding Summary ($ in Millions)

N/A

### Remarks

## D. Acquisition Strategy

N/A

## E. Performance Metrics

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

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| COST ($ in Millions) | Prior Years | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total | FY 2017 | FY 2018 | FY 2019 | FY 2020 | Cost To Complete | Total Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY* | - | 172.063 | 179.947 | 208.957 | - | 208.957 | 240.177 | 245.501 | 249.833 | 254.923 | - | - |

## A. Mission Description and Budget Item Justification

The Information Assurance and Survivability project is developing the core computing and networking technologies required to protect DoD's information, information infrastructure, and mission-critical information systems. The technologies will provide cost-effective security and survivability solutions that enable DoD information systems to operate correctly and continuously even under attack. Technologies developed under this project will benefit other projects within this program element as well as projects in the Command, Control, and Communications program element (PE 0603760E), the Network-Centric Warfare Technology program element (PE 0603766E), the Sensor Technology program element (PE 0603767E), and other projects that require secure, survivable, network-centric information systems.

| B. Accomplishments/Planned Programs ($ in Millions) | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| ***Title:*** High Assurance Cyber Military Systems | 23.889 | 24.000 | 34.500 |

***Description:*** The High Assurance Cyber Military Systems program will develop and demonstrate technologies to secure mission-critical embedded computing systems. The DoD is making increasing use of networked computing in systems such as military vehicles, weapon systems, ground sensors, smartphones, personal digital assistants, and other communication devices. This dependence makes it critically important that the embedded operating system provides high levels of inherent assurance. This operating system must also integrate the computational, physical, and networking elements of the system while running on a processor with very limited size, weight, and power. Consequently, it can only devote a limited share of its computational resources to security while satisfying hard real-time constraints. Recent advances in program synthesis, formal verification techniques, low-level and domain-specific programming languages, and operating systems mean that fully verified operating systems for embedded devices may be within reach at reasonable costs. The program will develop, mature, and integrate these technologies to produce an embedded computing platform that provides a high level of assurance for mission-critical military applications.

***FY 2014 Accomplishments:***
- Demonstrated compositionality, which is the ability to construct high assurance systems out of high assurance components.
- Extended the core high-assurance embedded operating system with additional functionality, including automatically generated device drivers and communication protocols.
- Automatically synthesized correct-by-construction control systems from high-level specifications.

***FY 2015 Plans:***

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Formally verify full functional correctness for the extended core operating system and the automatically synthesized control systems for selected vehicles.<br>- Demonstrate required security properties that follow from correctness for the extended core operating system and the automatically synthesized control systems.<br>- Perform static and dynamic assessments after modifications are made on militarily-relevant vehicles to evaluate the effectiveness of the synthesis and formal methods tools.<br>***FY 2016 Plans:***<br>- Apply an architecture-based approach to high-assurance system development to develop a large fraction of the software for a two-processor open-source quadcopter, a helicopter, an unmanned ground vehicle, and an American-built car.<br>- Demonstrate machine-tracked assurance cases for at least six system-wide security properties on targeted vehicles.<br>- Evaluate the effectiveness of approaches by having a red team conduct penetration-testing exercises on the targeted vehicles.<br>- Increase the level of automation of proof generation in theorem provers. | | | |
| ***Title:*** Vetting Commodity Computing Systems for the DoD (VET)<br>***Description:*** The Vetting Commodity Computing Systems for the DoD (VET) program will develop tools and methods to uncover backdoors and other hidden malicious functionality in the software and firmware on commodity IT devices. The international supply chain that produces the computer workstations, routers, printers, and mobile devices on which DoD depends provides many opportunities for our adversaries to insert hidden malicious functionality. VET technologies will also enable the detection of software and firmware defects and vulnerabilities that can facilitate adversary attack.<br>***FY 2014 Accomplishments:***<br>- Developed relevant application programming interfaces and defined formal semantics for the programming languages to be analyzed.<br>- Produced initial prototype attack scenario generation, program analysis, and diagnostic tools.<br>- Produced initial set of challenge programs for use in a competitive evaluation.<br>- Performed a competitive engagement between research and adversarial challenge performers to produce measurements of research progress against program metrics.<br>***FY 2015 Plans:***<br>- Improve the effectiveness of prototype tools, in particular by reducing the rates of false alarms and missed detections, through further competitive engagements.<br>- Expand the set of challenge programs to explore more complex forms of malicious hidden functionality including race conditions, information leakage, and defective encryption. | 17.954 | 21.760 | 30.325 |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Replace initial experimental platforms with more complex devices that are more operationally representative.<br>***FY 2016 Plans:***<br>- Use measurements against the program metrics, probabilities of false and missed detection and human analysis time, to identify the new techniques that are likely candidates for integration into an end-to-end DoD vetting application.<br>- Initiate development of an integrated vetting application that incorporates the most promising new techniques and scales to problems of operationally relevant size.<br>- Conduct an integrated end-to-end software/firmware-vetting technology demonstration relevant to potential transition partners. | | | |
| ***Title:*** Supply Chain Hardware Intercepts for Electronics Defense (SHIELD)<br>***Description:*** Counterfeit electronic parts are becoming ubiquitous, and pose a threat to the integrity and reliability of DoD systems. Detection of counterfeit components by current means is expensive, time-consuming, and of limited effectiveness. Maintaining complete control of the supply chain using administrative controls incurs substantial costs and has limitations. Current methods of detection involve a wide variety of techniques ranging from functional testing to physical inspections which may still miss certain classes of counterfeits. There have also been attempts by the semiconductor market to protect electronic components through the use of technology embedded in the component or its packaging. However, most methods are specific to a manufacturer's component and as such address only those issues deemed critical to that manufacturer. Some methods can be circumvented, or require slow, expensive, off-site forensic analysis to verify authenticity.<br>The Supply Chain Hardware Intercepts for Electronics Defense (SHIELD) program, leveraging and expanding on previous activities in the IRIS program, will develop a technology capable of confirming, at any time, the authenticity of once-trusted parts, even after they have transited a complex global supply chain. SHIELD will prevent counterfeit component substitution by incorporating a small, inexpensive additional silicon chip ("dielet") within the Integrated Circuit (IC) package. The dielet will provide a unique and encrypted ID as well as anti-tamper features. The microscopic-size dielet embedded in the electronic component packaging will be inductively powered and scanned by an authentication induction coil brought into very close proximity to the packaged chip, thus allowing for verification of chip identity.<br>***FY 2014 Accomplishments:***<br>- Defined dielet power consumption and transaction timing specifications.<br>- Defined physical form factor for dielet.<br>- Defined concept of operation for dielet to server communications.<br>- Selected target encryption standard for dielet.<br>***FY 2015 Plans:***<br>- Develop behavioral models for SHIELD dielet performance | 5.000 | 17.250 | 27.000 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Establish a power budget for all dielet electronics.<br>- Define server communication protocols, encryption scheme, and network architectures.<br>- Develop proof of concept for sensor, power and communications technologies.<br>- Design surrogate dielet for package tests.<br>- Define process modifications needed to accommodate SHIELD insertions.<br>- Develop technologies to allow secure key and ID storage and prevent tampering with the dielet.<br>- Design a compact encryption engine that enables a very small, low power, and low-cost dielet.<br>- Simulate and prototype dielet package-insertion techniques for placing SHIELD dielet on product.<br>***FY 2016 Plans:***<br>- Build prototype hardware.<br>- Develop infrastructure needed to execute SHIELD concept of operations.<br>- Design and build network appliance needed for remote interrogation of components. | | | |
| ***Title:*** Active Cyber Defense (ACD)<br>***Description:*** The Active Cyber Defense (ACD) program will enable DoD cyber operators to fully leverage our inherent home field advantage when defending the DoD cyber battlespace. In the cyber environment, defenders have detailed knowledge of, and unlimited access to, the system resources that attackers wish to gain. The ACD program will exploit emerging technologies to facilitate the conduct of defensive operations that involve immediate and direct engagement between DoD cyber operators and sophisticated cyber adversaries. Through these active engagements, DoD cyber defenders will be able to more readily disrupt, counter, and neutralize adversary cyber tradecraft in real time. Moreover, ACD-facilitated operations should cause adversaries to be more cautious and increase their work factor by limiting success from their efforts.<br>***FY 2014 Accomplishments:***<br>- Developed techniques for countering adversary cyber tradecraft and implemented early prototype software applications.<br>- Developed detailed system designs and design documentation.<br>- Finalized test plans and performed initial evaluations of active cyber defense prototypes in risk reduction assessments.<br>- Provided capabilities to support exercises with transition partners and to perform preliminary operational assessments of technologies.<br>***FY 2015 Plans:***<br>- Complete development of system components.<br>- Begin integration of technologies into complete prototype platforms.<br>- Test integrated capabilities.<br>***FY 2016 Plans:*** | 12.500 | 13.828 | 13.914 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Complete integration of system platforms and demonstrate capabilities to transition partners.<br>- Perform final test and evaluation of integrated capabilities and obtain approval for operational deployment.<br>- Support initial operational fielding of capability to facilitate transition to DoD cyber operators. | | | |
| ***Title:*** Mission-oriented Resilient Clouds (MRC) | 21.571 | 15.892 | 14.627 |

***Description:*** The Mission-oriented Resilient Clouds (MRC) program will create technologies to enable cloud computing systems to survive and operate through cyber attacks. Vulnerabilities found in current standalone and networked systems can be amplified in cloud computing environments. MRC will address this risk by creating advanced network protocols and new approaches to computing in potentially compromised distributed environments. Particular attention will be focused on adapting defenses and allocating resources dynamically in response to attacks and compromises. MRC will create new approaches to measuring trust, reaching consensus in compromised environments, and allocating resources in response to current threats and computational requirements. MRC will develop new verification and control techniques for networks embedded in clouds that must function reliably in complex adversarial environments.

***FY 2014 Accomplishments:***

- Produced a cloud task allocation system that maximizes mission effectiveness in the context of current system loads without significantly increasing hardware costs.
- Implemented and evaluated a packet-level monitoring tool that enables flexible, on-the-fly path analysis for network troubleshooting and attack detection.
- Validated and deployed an intrusion-tolerant overlay network for cloud monitoring and control.
- Transitioned a minimalist library microkernel into open source and commercial hypervisor products.
- Evaluated a network path diversity research product for potential transition into USPACOM distributed computing environments.

***FY 2015 Plans:***

- Demonstrate automated construction of diverse, redundant network flow paths that maximize communication resilience in clouds.
- Evaluate the scalability and resilience of a high-assurance cloud computing application development library in terms of number of concurrent replicas supported and volume of data handled.
- Develop and demonstrate hardened network services through fine-grained memory access controls that determine what valid memory addresses are read or written to by each instruction in a program.
- Insert MRC technologies into USPACOM distributed computing environments.
- Evaluate technologies in Defense Information Systems Agency (DISA) testbeds to facilitate transitions into DoD clouds.

***FY 2016 Plans:***

- Demonstrate correct, disruption-free upgrading of software defined networking controllers in live networks.

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Complete transition of one or more technologies into operational use by USPACOM and DISA. | | | |
| ***Title:*** Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)*<br>***Description:*** *Previously Secure Distributed Dynamic Computing (SDDC) funded in PE 0603766E, Project NET-01<br>The Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT) program will enable reliable communications for military forces that operate in disrupted/disadvantaged, intermittent, high-latency environments. The program will create algorithms and software prototypes for use exclusively at the network edge, specifically, on end hosts and/or on proxy servers (middleboxes) fronting groups of such end hosts within a user enclave. EdgeCT systems will sense and respond rapidly to network failures and attacks by dynamically adapting protocols utilized to exchange packets among these hosts, thereby implementing work-arounds (fight-through strategies) that restore networked communication. This will enable highly reliable networked communication for the military in the face of a wide variety of common network failure modes as well as cyber attacks against network infrastructure. EdgeCT technologies will be developed in collaboration with and transitioned to operational commands.<br>***FY 2015 Plans:***<br>- Develop a host-based architecture for reliable communications in disrupted/disadvantaged, intermittent, high-latency military environments.<br>- Develop techniques to sense and respond rapidly to network failures and attacks by dynamically adapting protocols utilized to exchange packets among hosts.<br>- Explore modes of user interaction and system concepts of operation with one or more operational commands.<br>***FY 2016 Plans:***<br>- Initiate development of software prototypes suitable for laboratory experimentation with operational commands.<br>- Develop work-arounds (fight-through strategies) that rapidly restore networked communication in the face of a wide variety of common network failure modes as well as cyber attacks against network infrastructure.<br>- Bring software prototypes to an initial field experiment in collaboration with an operational command. | - | 11.000 | 22.000 |
| ***Title:*** Cyber Fault-tolerant Attack Recovery (CFAR)<br>***Description:*** Building upon previous work in the Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program, the Cyber Fault-tolerant Attack Recovery (CFAR) program will develop novel architectures to achieve cyber fault-tolerance with commodity computing technologies. Current approaches to handling cyber-induced faults in mission-critical systems are inadequate, as perimeter defenses wrapped around vulnerable monocultures do not scale, while zero-day exploits evade signature-based defenses. The proliferation of processing cores in multi-core central processing units provides the opportunity to adapt fault-tolerant architectures proven in aerospace applications to mission-critical, embedded, and real-time computing | - | 10.000 | 20.149 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| systems. The CFAR program will combine techniques for detecting differences across functionally replicated systems with novel variants that guarantee differences in behavior under attack. The resulting CFAR-enabled computing systems will quickly detect deviations in processing elements at attack onset and rapidly reboot to restore affected services.<br>***FY 2015 Plans:***<br>- Formulate novel architectures that achieve cyber fault-tolerance with commodity computing technologies without requiring changes to the system concept of operations.<br>- Develop techniques for detecting differences across functionally replicated systems.<br>- Develop novel variants that guarantee differences in behavior under attack.<br>***FY 2016 Plans:***<br>- Demonstrate functionally replicated systems and novel variants that provide performance close to optimal and exhibit sufficient variability to guarantee differences in behavior under attack.<br>- Implement and test techniques for quickly detecting differences across replicated systems.<br>- Implement and evaluate alternative architectures for achieving cyber fault-tolerance for mission-critical military applications with commodity computing technologies.<br>- Work with potential transition sponsors to evaluate military computing systems as candidates for technology refresh with CFAR technologies. | | | |
| ***Title:*** Adaptable Information Access and Control (AIAC)<br>***Description:*** The Adaptable Information Access and Control (AIAC) program will create the capability to dynamically, flexibly, and securely share highly selective information across enterprise boundaries. In the civilian sphere, there is a recognized need for technologies that limit the sharing of information between commercial entities and U.S. government agencies to the greatest extent possible consistent with national security requirements. Similarly, the U.S. military is increasingly involved in humanitarian operations that require highly selective sharing of data with a heterogeneous mix of allies, coalition partners, and other stakeholders. AIAC will create confidentiality, privacy, multi-level security, discretionary access control, and policy engine technologies to allow tailored access to specific data and analytic results but not an entire database/file system/corpus. AIAC is timely due to recent progress on cryptographic techniques such as homomorphic encryption, secure multiparty computation, and differential privacy. Additional technologies that will be developed and incorporated include automated policy-driven releasability assessment and redaction, tactical obfuscation, and time-limited-access controls. The program will address the diverse and stringent legal and ethical requirements related to security, privacy, authentication, authorization, auditing, monitoring, access, and control encountered in both civilian and military environments. To facilitate deployment, AIAC technologies will be designed to work with the virtualization, cloud computing, and software-defined networking technologies now widely used in both civilian and military environments. | - | 7.093 | 17.600 |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| ***FY 2015 Plans:***<br>- Formulate access control schemes appropriate for diverse civilian, intelligence, law enforcement, and coalition use cases with particular focus on privacy-preserving analytics.<br>- Architect an access control policy engine for seamless interoperability with common computing and networking infrastructure software.<br>- Create technologies for confidentiality, privacy, multi-level security, discretionary access controls, automated policy-driven releasability assessment and redaction, tactical obfuscation, computing on encrypted data, and time-limited-access controls.<br>***FY 2016 Plans:***<br>- Implement access control software prototypes with flexibility adequate to support diverse civilian, intelligence, law enforcement, and coalition use cases and with scalability adequate for big data applications.<br>- Develop an access control policy engine and demonstrate interoperability with common cloud computing and software-defined networking infrastructure and services as appropriate.<br>- Evaluate and refine technologies for confidentiality, privacy, multi-level security, discretionary access controls, automated policy-driven releasability assessment and redaction, tactical obfuscation, computing on encrypted data, and time-limited-access controls. | | | |
| ***Title:*** Protecting Cyber Physical Infrastructure (PCPI)<br>***Description:*** * Formerly Protecting Cyber Physical Systems (PCPS)<br>The Protecting Cyber Physical Infrastructure (PCPI) program will create new technologies for ensuring the availability and integrity of critical U.S. cyber-physical infrastructure. The near-ubiquitous use of computers to monitor and control U.S. civilian and military critical infrastructure and the dependence of our society on electric power, clean water, waste processing, petroleum refining, chemical production, and other utilities/industries make this a national security issue. PCPI will develop technologies to monitor heterogeneous distributed control system networks, detect anomalies that require rapid assessment, and mitigate sensor spoofing and denial of service attacks. Hardware-in-the-loop simulation techniques will be developed to enable the discovery of emergent vulnerabilities and the development and optimization of mitigation strategies. This will include understanding the potential role of electric power markets in propagating or damping power grid anomalies. PCPI technologies will transition to military installations and commercial industry.<br>***FY 2015 Plans:***<br>- Create a hardware-in-the-loop simulation capability to enable the discovery of emergent vulnerabilities and the development and optimization of mitigation strategies. | - | 7.525 | 17.513 |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Formulate resilient architectures for real-time monitoring, analysis, and assessment of distributed industrial control systems and physical infrastructure.<br>- Investigate rapid re-provisioning techniques to quickly re-deploy firmware and operating system images to restore compromised devices back to a pristine, known state of operation.<br>***FY 2016 Plans:***<br>- Develop technologies to monitor heterogeneous distributed industrial control system networks, detect anomalies that require rapid assessment, and mitigate sensor spoofing and denial of service attacks.<br>- Extend simulation capabilities to understand the potential role of electric power markets in propagating or damping power grid anomalies.<br>- Develop techniques that use organic sensors, remote instrumentation, and other sources of cyber situation awareness information to continuously optimize cyber defenses.<br>- Explore defensive measures/counter-measures that can mitigate/thwart a coordinated cyber attack on national critical infrastructure. | | | |
| ***Title:*** Cyber Grand Challenge (CGC)<br>***Description:*** The Cyber Grand Challenge (CGC) program will create automated defenses that can identify and respond to cyber attacks more rapidly than human operators. CGC technology will monitor defended software and networks during operations, reason about flawed software, formulate effective defenses, and deploy defenses automatically. Technologies to be developed and integrated may include anomaly detection, Monte Carlo input generation, case-based reasoning, heuristics, game theory, and stochastic optimization. The CGC capability is needed because highly-scripted, distributed cyber attacks exhibit speed, complexity, and scale that exceed the capability of human cyber defenders to respond in a timely manner. DARPA will incentivize competition through a Grand Challenge in which CGC technologies compete head-to-head. Principal funding for this effort is provided in Project IT-05. Additional funding is being provided in IT-03 to enable the creation of the more robust competition infrastructure necessary to accommodate the large number of competitors.<br>***FY 2015 Plans:***<br>- Create a robust competition infrastructure as required to accommodate the large number of competitors.<br>***FY 2016 Plans:***<br>- Conduct world's first automated computer security contest: Cyber Grand Challenge Final Event.<br>- Release event results as cyber research corpus to measure and challenge future automated cyber capabilities. | - | 6.233 | 11.329 |
| ***Title:*** Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) | 19.626 | 11.182 | - |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| ***Description:*** The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program will develop cyber security technologies using the mechanisms of biological systems as inspiration for radically re-thinking basic hardware and system designs. Higher level organisms have two distinct immune systems: the innate system is fast and deadly but is only effective against a fixed set of pathogens; the adaptive system is slower, but can learn to recognize novel pathogens. Similarly, CRASH will develop mechanisms at the hardware and operating system level that eliminate known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH will also develop software techniques that allow a computer system to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH will develop techniques that make each computer system appear unique to the attacker and allow each system to change over time.<br><br>***FY 2014 Accomplishments:***<br>- Completed the implementation of three novel, secure processors, developed the associated security extensions to one operating system, and subjected each to independent red-team assessment.<br>- Demonstrated the capability to wrap integrated defense software and protect it from cyber attacks launched by an independent red team.<br>- Demonstrated the ability of two or more complete systems to block, survive, and recover from multiple attacks and automatically repair vulnerabilities.<br>- Developed and implemented multiple technologies for adding diversity to applications and assessed the impacts of these technologies on security and performance.<br>- Automatically produced diverse instantiations of one complete operating system and multiple large applications for multiple operating systems.<br>***FY 2015 Plans:***<br>- Deliver a hardened web server and browser that enable the creation of secure web applications from untrusted code.<br>- Demonstrate policy-based application monitoring and hardware-assisted self-healing of multiple applications.<br>- Demonstrate hardware-based detection of malicious software. | | | |
| ***Title:*** Rapid Software Development using Binary Components (RAPID)<br><br>***Description:*** The Rapid Software Development using Binary Components (RAPID) program will develop a system to identify and extract software components for reuse in new applications. The DoD has critical applications that must be ported to future operating systems. In many cases, the application source code is no longer available requiring these applications to continue to run on insecure and outdated operating systems, potentially impacting operations. Advanced technology research for the program is budgeted in PE 0603760E, Project CCC-04. | 8.198 | 10.396 | - |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| ***FY 2014 Accomplishments:***<br>- Fully integrated technologies into a single architecture and standardized interfaces to enable partners to interoperate with the system.<br>- Developed a single user interface that combines technical area views for monitoring system performance with a constructive interface for specifying desired products.<br>***FY 2015 Plans:***<br>- Develop new software component reuse capabilities to extend application performance to a wider range of realistic scenarios and enable an expanded concept of operations.<br>- Implement new capabilities in modules designed to interoperate seamlessly with deployed RAPID prototype systems.<br>- Integrate new modules into prototype RAPID systems deployed at transition partner sites and support initial operations. | | | |
| ***Title:*** Anomaly Detection at Multiple Scales (ADAMS)<br>***Description:*** The Anomaly Detection at Multiple Scales (ADAMS) program will develop and apply algorithms for detecting anomalous, threat-related behavior of systems, individuals, and groups over hours, days, months, and years. ADAMS will develop flexible, scalable, and highly interactive approaches to extracting actionable information from information system log files, sensors, and other instrumentation. ADAMS will integrate these anomaly detection algorithms to produce adaptable systems for timely insider threat detection.<br>***FY 2014 Accomplishments:***<br>- Created the capability to incorporate direct user feedback to improve coverage of threat types.<br>- Developed and implemented technology that is adaptable to a wide variety of organizational structures, workflows, and data sources.<br>- Developed techniques to provide the evidence needed to initiate focused response activities.<br>- Developed two integrated prototype anomaly/threat detection systems suitable for rapid deployment in an operational environment.<br>***FY 2015 Plans:***<br>- Develop and implement technology to capture analyst expertise for assessing and explaining detected anomalies and incorporate such user feedback in decision loops for operators without highly specialized computer science knowledge.<br>- Harden prototype and obtain DoD Information Assurance Certification and Accreditation Process approval for use on military networks.<br>- Conduct and evaluate initial prototype in a large scale environment with operational partners. | 15.272 | 7.000 | - |
| ***Title:*** Active Authentication | 13.100 | 7.025 | - |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|

***Description:*** The Active Authentication program will develop more effective user identification and authentication technologies. Current authentication approaches are typically based on long, complex passwords and incorporate no mechanism to verify the user originally authenticated is the user still in control of the session. The Active Authentication program will address these issues by focusing on the unique aspects of the individual (i.e., the cognitive fingerprint) through the use of software-based biometrics that continuously validate the identity of the user. Active Authentication will integrate multiple biometric modalities to create an authentication system that is accurate, robust, and transparent to the user.

***FY 2014 Accomplishments:***
- Demonstrated enhanced authentication using multiple biometrics representing complementary aspects of the individual.
- Evaluated the level of confidence that is achievable using multiple advanced authentication mechanisms and quantified the resulting level of security using red teaming and other techniques.
- Prototyped an authentication platform suitable for DoD use in collaboration with potential transition sponsors.
- Initiated development of multiple authentication biometrics suitable for deployment on mobile hardware for potential use by the DoD.

***FY 2015 Plans:***
- Demonstrate multiple authentication biometrics suitable for deployment on mobile hardware for potential use by the DoD.
- Prove flexibility of underlying prototype platform by creating an additional authentication platform suitable for DoD.
- Prototype an authentication platform suitable for use on mobile hardware in collaboration with potential transition sponsors.

| | | | |
|---|---|---|---|
| ***Title:*** Safer Warfighter Computing (SAFER) | 15.150 | 4.066 | - |

***Description:*** The Safer Warfighter Computing (SAFER) program is creating a technology base for assured and trustworthy Internet communications and computation, particularly in untrustworthy and adversarial environments. SAFER creates automated processes and technologies to enable military users to send and receive content on the Internet, utilizing commercially available hardware and software, in ways that avoid efforts to deny, locate, or corrupt communications. SAFER is also developing technology for performing computations on encrypted data without decrypting it first through fully homomorphic encryption and interactive, secure multi-party computation schemes. This will enable, for example, the capability to encrypt queries and compute an encrypted search result without decrypting the query. This technology will advance the capability to run programs on untrusted hardware while keeping programs, data, and results encrypted and confidential. This mitigates the important aspect of supply chain compromise.

***FY 2014 Accomplishments:***
- Improved software performance in fully homomorphic encryption, garbled-circuit secure multiparty computation, and secret-sharing secure multiparty computation, and performed independent benchmarks.

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Demonstrated an additional two orders of magnitude improvement in the performance of fully homomorphic encryption.<br>- Refined field programmable gate array implementation of fully homomorphic encryption to yield a further order of magnitude performance improvement over optimized software implementation.<br>- Demonstrated safe, encrypted Internet communications application: secure Voice over Internet Protocol (VOIP) teleconferencing.<br>***FY 2015 Plans:***<br>- Develop improved decoy routing, parallelized group messaging, dynamic traffic camouflage, and rendezvous strategy technologies.<br>- Further optimize field programmable gate array and software implementations of fully homomorphic encryption to double performance over prior implementations.<br>- Conduct the final independent, adversarial assessment of the effectiveness of technologies to prevent communication localization and detection, including newly developed adversarial techniques. | | | |
| ***Title:*** Integrated Cyber Analysis System (ICAS)<br>***Description:*** The Integrated Cyber Analysis System (ICAS) program will develop techniques to automatically discover probes, intrusions, and persistent attacks on enterprise networks. At present, discovering the actions of capable adversaries requires painstaking forensic analysis of numerous system logs by highly skilled security analysts and system administrators. ICAS will develop technologies to facilitate the correlation of interactions and behavior patterns across all system data sources and thereby rapidly uncover aberrant events and detect system compromise. This includes technologies for automatically representing, indexing, and reasoning over diverse, distributed, security-related data and system files.<br>***FY 2014 Accomplishments:***<br>- Developed a multi-tiered approach to device identification and information extraction by transcoding Simple Protocol and Resource description framework Query Language (SPARQL).<br>- Developed SQL transcoding support to enable Relational Database Management System (RDBMS) information extraction.<br>- Conducted initial demonstrations of core technologies including automatic indexing of data sources, common language integration, and reasoning across federated databases.<br>***FY 2015 Plans:***<br>- Develop and implement algorithms for automatically identifying and quantifying specific security risks on enterprise networks.<br>- Conduct initial technology demonstrations including automatic indexing of data sources, common language integration, and reasoning across federated databases.<br>- Integrate, evaluate, and optimize algorithms via testing against attacks/persistent threats provided by transition partners. | 10.000 | 3.000 | - |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 / *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Complete fully functional beta versions of the applications with operational stability suitable for testing at transition partner locations. | | | |
| ***Title:*** Logan<br>***Description:*** The Logan program will provide DoD enhanced capabilities to conduct Computer Network Attack (CNA). Techniques will be developed to disrupt and degrade adversary information systems and network operations, with particular interest in techniques likely to be robust to adversary countermeasure strategies.<br>***FY 2014 Accomplishments:***<br>- Automated and tested prototypes in conjunction with transition partner.<br>- Optimized and hardened prototypes and initiated transition.<br>***FY 2015 Plans:***<br>- Transition automated prototype system. | 8.803 | 2.697 | - |
| ***Title:*** Integrity and Reliability of Integrated CircuitS (IRIS)<br>***Description:*** Integrated circuits (ICs) are core components of most electronic systems developed for the Department of Defense. However, the DoD consumes a very small percentage of the total IC production in the world. As a result of the globalization of the IC marketplace, much of the advanced IC production has moved to offshore foundries, and these parts make up the majority of ICs used in today's military systems.<br>Without the ability to influence and regulate the off-shore fabrication of ICs, there is a risk that parts acquired for DoD systems may not meet stated specifications for performance and reliability. This risk increases considerably with the proliferation of counterfeit ICs in the marketplace, as well as the potential for the introduction of malicious circuits into a design.<br>The Integrity and Reliability of Integrated CircuitS (IRIS) program developed techniques that will provide electronic system developers the ability to validate the function of digital, analog and mixed-signal ICs non-destructively, given limited data about the chip's detailed design specifications. These techniques included advanced imaging for identification of functional elements in deep sub-micrometer Complementary Metal-Oxide Semiconductor (CMOS) circuits, as well as computational methods to deal with the extremely difficult problem of determining device connectivity.<br>Finally, the IRIS program developed innovative methods to determine the reliability of an IC by testing a limited number of samples. The current understanding of IC aging mechanisms, including negative bias temperature instability (NBTI), hot carrier injection (HCI), time-dependent dielectric breakdown (TDDB) and electromigration (EM) was leveraged to develop unique diagnostic test techniques. | 1.000 | - | - |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-03 **/** *INFORMATION ASSURANCE AND SURVIVABILITY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| ***FY 2014 Accomplishments:***<br>- Exercised completed methods for non-destructive imaging, circuit extraction and functional derivation.<br>- Demonstrated methods for reliability analysis for improved accuracy, functionality and efficacy.<br>- Combined analysis methods for imaging, circuit extraction and reliability modeling to identify anomalies on an integrated circuit test article, and to determine the impact of those anomalies on the reliability of the test article.<br>- Transitioned technology to the Navy and the Air Force Research Lab for deployment in existing programs to analyze circuits for counterfeit issues.<br>- Completed testing and evaluation of performers and test chips by government virtual lab highlighting advancements in program closeout and gaps to be addressed. | | | |
| **Accomplishments/Planned Programs Subtotals** | 172.063 | 179.947 | 208.957 |

**C. Other Program Funding Summary ($ in Millions)**

N/A

**Remarks**

**D. Acquisition Strategy**

N/A

**E. Performance Metrics**

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

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-04 / *LANGUAGE TECHNOLOGY* |

| COST ($ in Millions) | Prior Years | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total | FY 2017 | FY 2018 | FY 2019 | FY 2020 | Cost To Complete | Total Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT-04: *LANGUAGE TECHNOLOGY* | - | 74.332 | 45.511 | 60.897 | - | 60.897 | 65.240 | 51.477 | 54.856 | 54.755 | - | - |

**A. Mission Description and Budget Item Justification**

The Language Technology project will develop human language technologies to provide critical capabilities for a wide range of national security needs ranging from knowledge management to low-resource language understanding. Foreign-language news broadcasts, web-posted content, and foreign-language hard-copy documents could provide insights regarding regional and local events, attitudes and activities, if there was a system that could automatically process large volumes of speech and text in multiple languages obtained through a variety of means. The project develops technologies to automatically translate, collate, filter, synthesize, summarize, and present relevant information in timely and relevant forms. In addition, current U.S. military operations often require warfighters on the ground to understand speech and text in foreign languages for which there may be no available linguists. The Language Technology project is addressing these diverse requirements by developing core language processing technologies and integrating these technologies into operational prototypes suitable for use in the field.

| **B. Accomplishments/Planned Programs ($ in Millions)** | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| ***Title:*** Deep Exploration and Filtering of Text (DEFT) | 28.369 | 28.333 | 30.223 |
| ***Description:*** The Deep Exploration and Filtering of Text (DEFT) program will enable automated extraction, processing, and inference of information from text in operationally relevant application domains. A key DEFT emphasis is to determine explicit and implicit meaning in text through probabilistic inference, anomaly detection, and other techniques. To accomplish this, DEFT will develop and apply formal representations for basic facts, spatial, temporal, and associative relationships, causal and process knowledge, textually entailed information, and derived relationships and correlated actions/events. DEFT inputs may be in English or in a foreign language and sources may be completely free-text or semi-structured reports, messages, documents, or databases. DEFT will extract knowledge at scale for open source intelligence and threat analysis. Planned transition partners include the intelligence community and operational commands.<br>***FY 2014 Accomplishments:***<br>- Developed initial methods and algorithms for reasoning about both explicitly and implicitly expressed opinions and beliefs, for extracting causal knowledge, and for finding implicit meaning based on anomalous usages and disfluencies in a document or set of documents.<br>- Conducted performance evaluations on data sets related to event representation and inference.<br>- Expanded capabilities to additional application problems and domains such as target information augmentation in collaboration with end-users. | | | |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-04 / *LANGUAGE TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Demonstrated feasibility of deep extraction and filtering for selected end-user applications and transitioned initial sets of algorithms to the intelligence community and a Combatant Command.<br>***FY 2015 Plans:***<br>- Develop technology for extracting belief, sentiment, and intent; for representing geo-spatial features and temporal events; and for inference and alerting from a set of documents.<br>- Integrate multiple complementary algorithms into a comprehensive and consistent functional suite to support end-user workflows and problems.<br>- Increase algorithm development focus towards knowledge base representation in preparation for embedding algorithms in workflows to enable reasoning and downstream analysis.<br>- Extend algorithms to additional foreign languages such as Spanish and Chinese.<br>- Conduct performance evaluations on data sets related to event representation, anomaly detection, and knowledge base population.<br>- Transition algorithm suites and conduct effectiveness assessments at end-user sites.<br>- Enlarge the scope of event coverage to include increasingly complex events.<br>***FY 2016 Plans:***<br>- Improve algorithm performance on current functions and expand to new functions such as extending currently single-document algorithms to function across documents.<br>- Optimize algorithm coverage and improve performance for foreign languages such as Spanish and Chinese.<br>- Join and optimize combined output of algorithms focused on different tasks such as belief and sentiment extraction, event argument and attribute identification, and relation mapping.<br>- Transition system-level prototype to end-user site for effectiveness assessment.<br>- Refine areas of focus based on results of transition site evaluations and open evaluation performance. | | | |
| ***Title:*** Robust Automatic Translation of Speech (RATS)<br>***Description:*** The Robust Automatic Transcription of Speech (RATS) program is developing robust speech processing techniques for conditions in which speech signals are degraded by distortion, reverberation, and/or competing conversation. Robust speech processing technologies enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite a noisy or reverberant environment. Techniques of interest include speech activity detection, language identification, speaker identification, and keyword spotting. RATS technology is being developed and optimized on real world data in conjunction with several operational users.<br>***FY 2014 Accomplishments:*** | 4.850 | 6.178 | 8.500 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-04 **/** *LANGUAGE TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|

- Evaluated performance showing substantial progress on noisy and degraded speech signals from the program-generated data corpus.
- Collected and annotated classified field data for training and testing.
- Evaluated technologies on field-collected data and tested the system for in-the-field adaptation.
- Obtained real world data from operational users and performed testing on site at the user location.
- Established relationships with various DoD and intelligence community agencies as potential transition partners.

***FY 2015 Plans:***

- Develop new methods for field adaptations which include lightly supervised and unsupervised adaptation of the algorithms to new channels and environments.
- Develop methods for coping with extraneous signals found in field data.
- Develop techniques to significantly reduce the amount of data from hours to minutes for adapting algorithms to new channels.
- Produce a software integrated platform with a set of Application Programming Interfaces (APIs) and Graphical User Interfaces (GUIs) to be inserted at DoD and intelligence community partner sites and tested in the working environment of the partners.

***FY 2016 Plans:***

- Develop, integrate and test techniques to deal with multiple speakers and overlapping speaker channels.
- Collect and annotate additional field collected data.
- Integrate technologies in transition partner platforms, adjusting systems to fit partner needs.
- Evaluate technologies on specialized operational scenarios.

| ***Title:*** Low Resource Languages for Emergent Incidents (LORELEI)* | - | 11.000 | 22.174 |
|---|---|---|---|

***Description:*** *Formerly Foreign Language Rapid Response (FLRR)

The Low Resource Languages for Emergent Incidents (LORELEI) program will develop the capability to rapidly construct machine translation and other human language technologies for low-resource foreign languages. The United States military operates globally and frequently encounters low-resource languages, i.e., languages for which few linguists are available and no automated human language technology capability exists. Historically, exploiting foreign language materials required protracted effort, and as a result systems exist only for languages in widespread use and in high demand. The goal of the LORELEI program is to dramatically advance the state of computational linguistics and human language technology to enable rapid, low-cost development of language processing capabilities for low-resource languages. To achieve this LORELEI will eliminate reliance on huge, manually-translated, manually-transcribed, or manually-annotated corpora and instead will leverage language-universal resources, project from related-language resources, and fully exploit a broad range of language-specific resources. These capabilities will be exercised to provide situational awareness based on information from any language, in support of emergent

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-04 / *LANGUAGE TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| missions such as humanitarian assistance/disaster relief, terrorist attack response, peacekeeping, and infectious disease response.<br>***FY 2015 Plans:***<br>- Develop techniques for quantifying the linguistic similarity of language usage in diverse documents and media.<br>- Develop semantic techniques for identifying the common topics, themes, and sentiment in speech and text in diverse foreign languages.<br>- Explore techniques for optimizing combinations of existing resources to eliminate reliance on large parallel corpora in the context of exploiting foreign language sources in low-resource languages.<br>***FY 2016 Plans:***<br>- Develop algorithms to exploit the universal properties of languages when rapidly ramping up for a low-resource language.<br>- Collect, generate, and annotate data for an initial set of resources in typologically representative medium-resource languages.<br>- Create a baseline toolkit to rapidly develop an initial situational awareness capability given a new low-resource language document collection. | | | |
| ***Title:*** Broad Operational Language Translation (BOLT)<br>***Description:*** The Broad Operational Language Translation (BOLT) program enabled language processing of informal and dialectal genres. Historically, foreign language translation technology was geared toward formal content, like broadcast media and newswire, but did not address informal or dialectal genres. BOLT developed new approaches to automated language translation, human-machine multimodal dialogue, and language generation and applied these to informal genres such as online discussion groups, messaging, and telephone conversation. While Chinese and dialectal Arabic were the two languages addressed directly in BOLT, techniques developed for these two languages have wide applicability to other languages and dialects.<br>***FY 2014 Accomplishments:***<br>- Developed improved algorithms for translating two informal genres of Arabic and Chinese text, online discussion groups and messaging, to enable comprehension of colloquialisms and idiomatic speech and added a third genre, telephone conversation.<br>- Used methods developed for Egyptian dialectal Arabic to create databases, tools, and algorithms for additional Arabic dialects.<br>- Developed dialogue management techniques such as computer-moderated turn-taking to avoid divergence as an approach for improving the performance of bi-directional Arabic-English dialogue systems.<br>- Completed the annotated corpora of Arabic and Chinese informal genre data by adding new dialects and enhanced their utility by incorporating additional annotations. | 38.913 | - | - |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-04 / *LANGUAGE TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Formalized government purpose rights and transitioned software for translating informal genres of Arabic and Chinese to a Combatant Command and the Intelligence Community. | | | |
| ***Title:*** Multilingual Automatic Document Classification, Analysis and Translation (MADCAT)<br>***Description:*** The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program developed and integrated technology to enable exploitation of foreign language hand-written documents. This technology is crucial to the warfighter, as documents such as notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images captured in the field may contain extremely important time-sensitive information. The MADCAT program addressed this need by producing devices to convert such captured documents from Arabic into readable English in the field. MADCAT substantially improved applicable technologies, in particular document analysis and optical character recognition/ optical handwriting recognition. MADCAT integrated these improved technologies with translation technology and created prototypes for field trials.<br>***FY 2014 Accomplishments:***<br>- Fielded MADCAT to multiple Korean sites as an off-line capability for evaluation and routine use by end users.<br>- Evaluated performance of MADCAT in the end user environment showing substantial progress in machine translation of Korean to English and English to Korean on end user provided documents in exercises conducted on site.<br>- Distributed the MADCAT framework for access to the entire U.S. military on the Korean peninsula via the CENTRIX-K network and demonstrated the system during major annual combined U.S.-Korean Forces exercise Ulchi Freedom Guardian.<br>- Developed and deployed a new machine translation capability enabling model adaptation using onsite data and continued to enhance end user learning and recall capabilities with translation memory capabilities.<br>- Signed an MOU with the U.S. Army Chief of Staff in Korea which establishes responsibilities and commitments for MADCAT technology in Korea. | 2.200 | - | - |
| **Accomplishments/Planned Programs Subtotals** | 74.332 | 45.511 | 60.897 |

## C. Other Program Funding Summary ($ in Millions)

N/A

**Remarks**

## D. Acquisition Strategy

N/A

## E. Performance Metrics

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

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-05 / *CYBER TECHNOLOGY* |

| COST ($ in Millions) | Prior Years | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total | FY 2017 | FY 2018 | FY 2019 | FY 2020 | Cost To Complete | Total Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT-05: *CYBER TECHNOLOGY* | - | 57.767 | 69.149 | 35.014 | - | 35.014 | - | - | - | - | - | - |

## A. Mission Description and Budget Item Justification

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

| B. Accomplishments/Planned Programs ($ in Millions) | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| ***Title:*** Plan X | 35.599 | 43.419 | 25.150 |

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

***FY 2014 Accomplishments:***
- Created preliminary end-to-end system prototype that supports efficient network mapping, measurement, and network change detection applications.
- Hosted private cloud infrastructure with automated provisioning of computing resources on a standalone closed network that enables a massively distributed data and event store.
- Developed approaches to host Plan X control plane in a wide variety of network architectures using diverse scalable platforms.
- Designed and implemented first generation prototypes of the commander, planner, and operator views for the graphical user interface.
- Created automated network simulation technology to model the cyber battlespace, generate cyber warfare mission plans, and script cyber warfare missions using a domain specific language for programming at Internet scale.
- Collaborated with operators from Air Force, Navy, Marine Corps, and Army cyber components and U.S. Cyber Command.

***FY 2015 Plans:***
- Create runtime environment and platforms capable of supporting a large scale user base, massive-scale deployments, resiliency to failures of any system component, and managing high ingest rates.

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-05 **/** *CYBER TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Demonstrate cyber battle damage assessment from algorithmically placed vantage points.<br>- Demonstrate military network tactical situational awareness applications and use cases.<br>- Release Plan X 1.0 Alpha system and field test capabilities at military cyber exercises such as Cyber Flag and Red Flag.<br>- Conduct field tests of computer network operations scenario development and training capabilities.<br>- Create technical roadmap for transition to operational environment, including understanding of transition partner networks and integration points.<br>***FY 2016 Plans:***<br>- Release Plan X 1.0 Beta system and field test with military transition partners at cyber exercises such as Cyber Flag and Red Flag.<br>- Publish application store software development kit and integrate third party cyber capabilities.<br>- Demonstrate large-scale deployment of the end-to-end system with users and roles running on multiple devices in disparate locations.<br>- Integrate with existing military command and control/intel systems to allow bidirectional flow of data to and from Plan X to provide visualization and insights into the cyber battlespace.<br>- Develop and implement technologies for multi-level security access and use privileges.<br>- Integrate multi-level security access and use privileges and initiate technology transition with USCYBERCOM and Service components. | | | |
| ***Title:*** Cyber Grand Challenge (CGC)<br>***Description:*** The Cyber Grand Challenge (CGC) program will create automated defenses that can identify and respond to cyber attacks more rapidly than human operators. CGC technology will monitor defended software and networks during operations, reason about flawed software, formulate effective defenses, and deploy defenses automatically. Technologies to be developed and integrated may include anomaly detection, Monte Carlo input generation, case-based reasoning, heuristics, game theory, and stochastic optimization. The CGC capability is needed because highly-scripted, distributed cyber attacks exhibit speed, complexity, and scale that exceed the capability of human cyber defenders to respond in a timely manner. DARPA will incentivize competition through a Grand Challenge in which CGC technologies compete head-to-head. Additional funding for this effort is provided in Project IT-03.<br>***FY 2014 Accomplishments:***<br>- Developed host phase of instrumented competition framework for automated cyber defense.<br>- Initiated development of automated cyber defenders to identify flaws and formulate defenses.<br>- Conducted competitive assessments to identify the most promising technology solutions.<br>***FY 2015 Plans:*** | 10.438 | 16.832 | 9.864 |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E / *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-05 / *CYBER TECHNOLOGY* |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Extend development of automated cyber defenders to allow real time in situ network defense decision making.<br>- Develop a cyber research corpus using techniques from game theory, other quantitative disciplines, and emergent behavior.<br>- Conduct mid-term qualification evaluation of cyber technologies through competitive challenges.<br>***FY 2016 Plans:***<br>- Conduct world's first automated computer security contest: Cyber Grand Challenge Final Event.<br>- Release event results as cyber research corpus to measure and challenge future automated cyber capabilities. | | | |
| ***Title:*** Crowd Sourced Formal Verification (CSFV)<br>***Description:*** The Crowd-Sourced Formal Verification (CSFV) program will create technologies that enable crowd-sourced approaches to securing software systems through formal verification. Formal software verification is a rigorous method for proving that software has specified properties, but formal verification does not currently scale to the size of software found in modern weapon systems. CSFV will enable non-specialists to participate productively in the formal verification process by transforming formal verification problems into user-driven simulations that are intuitively understandable.<br>***FY 2014 Accomplishments:***<br>- Developed five web-based interactive computer simulations based on mapped high-level software specifications and codes.<br>- Launched and maintained public web site to attract the widest possible base for crowd-sourcing formal verifications.<br>- Applied simulations to large Java and C computer programs consisting of hundreds of thousands of lines of source code.<br>- Mapped solutions as code annotations back into formal verification tools and assessed the effectiveness of these solutions by verifying the absence of errors on the MITRE Common Weakness Enumeration/SANS Institute Top 25 lists.<br>- Refined initial simulations and began design and development of five new simulations for greater verification effectiveness.<br>***FY 2015 Plans:***<br>- Complete development of five new simulations.<br>- Refine simulations to make them accessible to a large set of non-specialists.<br>- Augment simulations to handle very large Java and C computer programs consisting of millions of lines of source code.<br>- Enhance public web site to include these new simulations.<br>- Assess effectiveness of the new simulations on the large-sized code targets. | 11.730 | 8.898 | - |
| **Accomplishments/Planned Programs Subtotals** | 57.767 | 69.149 | 35.014 |

## C. Other Program Funding Summary ($ in Millions)

N/A

**Remarks**

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Defense Advanced Research Projects Agency | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 **/** 2 | **R-1 Program Element (Number/Name)**<br>PE 0602303E **/** *INFORMATION & COMMUNICATIONS TECHNOLOGY* | **Project (Number/Name)**<br>IT-05 **/** *CYBER TECHNOLOGY* |

## D. Acquisition Strategy

N/A

## E. Performance Metrics

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