| | |
|---|---|
| **Exhibit R-2**, **RDT&E Budget Item Justification:** PB 2016 Office of the Secretary Of Defense | **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 0602668D8Z **/** *Cyber Security Research* |

| 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 | - | 11.637 | 14.979 | 13.727 | - | 13.727 | 12.966 | 15.249 | 15.537 | 15.748 | Continuing | Continuing |
| P003: *Cyber Applied Research* | - | 11.637 | 14.979 | 13.727 | - | 13.727 | 12.966 | 15.249 | 15.537 | 15.748 | Continuing | Continuing |

## A. Mission Description and Budget Item Justification

Our military forces require resilient, reliable networks and computer systems to conduct effective operations. However, the number and sophistication of threats in cyberspace are rapidly growing, making it critical to improve the cyber security of Department of Defense (DoD) systems to counter those threats and assure our missions. The Cyber Applied Research program focuses on innovative and sustained research in both cyber security and computer network operations to develop new concepts to harden key network and computer components, design new resilient cyber infrastructures, increase the military's ability to fight and survive during cyber attacks, disrupt nation-state level attack planning and execution, measure the state of cyber security, explore and exploit new ideas in cyber warfare for agile cyber operations and mission assurance, and protect tactical networks, weapons systems and platforms.

This program builds upon existing basic and applied research results. The program focuses on integrating computer network defense and computer network operations, addressing joint problems in cyber operations, and filling capability and technology gaps as identified in the 2012 Cyber Priority Steering Council Science and Technology (S&T) Roadmap, the 2013 Cyber S&T Capability Gap Framework and other assessments conducted by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)). Progress and results are reviewed by the DoD Cyber S&T Community of Interest. New efforts will also be aligned with emerging U.S. Cyber Command (USCYBERCOM) mission requirements.

## B. Program Change Summary ($ in Millions)

| | FY 2014 | FY 2015 | FY 2016 Base | FY 2016 OCO | FY 2016 Total |
|---|---|---|---|---|---|
| Previous President's Budget | 13.907 | 15.000 | 15.285 | - | 15.285 |
| Current President's Budget | 11.637 | 14.979 | 13.727 | - | 13.727 |
| Total Adjustments | -2.270 | -0.021 | -1.558 | - | -1.558 |
| • Congressional General Reductions | - | - | | | |
| • Congressional Directed Reductions | - | - | | | |
| • Congressional Rescissions | - | - | | | |
| • Congressional Adds | - | - | | | |
| • Congressional Directed Transfers | - | - | | | |
| • Reprogrammings | -1.807 | - | | | |
| • SBIR/STTR Transfer | -0.463 | - | | | |
| • FFRDC Sec 8104 | - | -0.021 | - | - | - |
| • Realignment for Higher Priority Programs | - | - | -1.516 | - | -1.516 |
| • Economic Assumptions | - | - | -0.042 | - | -0.042 |

| | |
|---|---|
| **Exhibit R-2**, **RDT&E Budget Item Justification:** PB 2016 Office of the Secretary Of Defense | **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 0602668D8Z **I** *Cyber Security Research* |

**Change Summary Explanation**

FY 2016 internal realignment reflects funding for higher Departmental priorities and requirements.

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602668D8Z / *Cyber Security Research* | **Project (Number/Name)**<br>P003 / *Cyber Applied Research* |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P003: *Cyber Applied Research* | - | 11.637 | 14.979 | 13.727 | - | 13.727 | 12.966 | 15.249 | 15.537 | 15.748 | Continuing | Continuing |

## A. Mission Description and Budget Item Justification

This program focuses on science and technology (S&T) to support integrating computer network defense and computer network operations, addressing joint challenges in cyber operations, and filling capability and technology gaps as identified in the Cyber Community of Interest S&T Roadmap, the 2013 Cyber S&T Capability Gap Framework and other assessments conducted by OASD(R&E). Progress and results are reviewed by the DoD Cyber S&T Community of Interest.

Beginning in FY 2013, the program expanded research in cyber command and control to provide warfighters and commanders new situational awareness, course of action analysis, cyber operational agility and cyber mission control. This research will include protection of tactical networks, weapons systems and platforms. Beginning in FY 2014, new efforts were aligned with emerging U.S. Cyber Command (USCYBERCOM) mission requirements.

The six technical thrust areas are:

Foundations of Trust
Resilient Infrastructure
Agile Operations
Assuring Effective Missions
Cyber Modeling, Simulation, and Experimentation (MSE)
Embedded, Mobile, and Tactical Environments (EMT)

## B. Accomplishments/Planned Programs ($ in Millions)

| | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| ***Title:*** Foundations of Trust | 4.295 | 1.005 | 1.437 |

***Description:*** Develop approaches and methods to establish known degrees of assurance that devices, networks, and cyber missions perform as expected, despite attack or error. This technical area encompasses all aspects of the assessment, establishment, propagation, maintenance, and composition of trust relationships between devices, networks, and people.

***FY 2014 Accomplishments:***
- Demonstrated a protection system that can prevent, detect, and respond to supply chain attacks.
- Demonstrated trusted computing platform with capabilities that can detect and mitigate compromise.
- Developed techniques to enable continuous measurement and integrity checking of operating system and mission application software during execution.

***FY 2015 Plans:***
- Develop a non-signature based capability to detect malicious code on cyber systems with high accuracy.

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Develop detection algorithms for malicious Universal Serial Bus (USB) firmware/hardware.<br>- Conduct theoretical Graphics Processing Unit (GPU) image processing research and conduct experimentation on production Scanning Electron Microscope (SEM) data.<br>***FY 2016 Plans:***<br>- Evaluate image processing computation developed in FY 2015 and identify those steps which might benefit from GPU acceleration.<br>- Build a SEM image processing-focused library of GPU tools. | | | |
| ***Title:*** Resilient Infrastructure<br>***Description:*** Entails the ability to withstand cyber attacks, and to sustain or recover critical functions. A resilient infrastructure has the ability to continue to perform its functions and provide its services at required levels during an attack. The objective in this area is to develop integrated architectures that are optimized for their ability to absorb (cyber) shock, and recover in a timely fashion to a known secure state with well-defined performance characteristics. Resilient Algorithms and Protocols address novel protocols and algorithms to increase the repertoire of resiliency mechanisms available to the infrastructure and architecture. Research is needed to develop resiliency at lower levels with specific algorithms and protocols to support higher-level resilient architectures.<br>***FY 2014 Accomplishments:***<br>- Developed verification and monitoring techniques to enhance security of deployed networks.<br>- Developed signal processing approaches and recent network theory advances to detect and predict adversary activities in networks.<br>- Conducted modeling and simulation that resulted in improved understanding and approaches for resiliency.<br>***FY 2015 Plans:***<br>- Design framework for secure modularization and virtualization of nodes and networks.<br>- Develop methods for increasing resiliency of large scale tactical networks while enabling increased mobility.<br>- Develop cyber resiliency techniques and tools against attacks on known classes of cyber vulnerabilities applicable to Cyber Physical Systems (CPS), and specifically, to hull, mechanical and electrical (HM&E).<br>***FY 2016 Plans:***<br>- Deploy capabilities on applicable CPS/HM&E systems.<br>- Design and develop capability to monitor and autonomously remove malicious code, commands and data. | 1.295 | 1.090 | 0.946 |
| ***Title:*** Agile Operations<br>***Description:*** Explore new methods and technologies to dynamically reshape cyber systems as conditions/goals change, in order to escape harm, or to manipulate the adversary. These capabilities present technology challenges in the areas of Autonomic | 2.030 | 0.500 | - |

| | | |
|---|---|---|
| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense | | **Date:** February 2015 |
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602668D8Z / *Cyber Security Research* | **Project (Number/Name)**<br>P003 / *Cyber Applied Research* |

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

Cyber Agility and Cyber Maneuver. Cyber Maneuver is a new way to manage systems dynamically in a cyber operation. It is a set of emerging methods for maintaining defensive or offensive advantage in cyber operations. It entails developing mechanisms that enable goal-directed reshaping of cyber systems. Cyber Maneuver encompasses reallocation for repurposing a device or platform, reconfiguration for changing the way a system performs a task, and repositories for altering the operating state in a logical or physical topology. Autonomic Cyber Agility covers several forms of agility e.g., as cyber infrastructures increase in scale and complexity, there is an urgent need for autonomous and agile mechanisms to reconfigure, heal, optimize, and protect defensive and offensive cyber mechanisms.

***FY 2014 Accomplishments:***

- Completed agility specifications to enable rapid integration and reduced acquisition/integration cost for the development of current and future cyber mission operations. Technology transitioned to classified program.
- Defined quantifiable metrics in which the DoD could build, buy, configure, and maintain network defensive capabilities to thwart certain classes of threats.

***FY 2015 Plans:***

- Design distributed systems architectures and service application polymorphism.
- Develop automated reasoning techniques for executing courses of action.

***FY 2016 Plans:***

- Projects concluding; working to transition efforts into relevant programs.

| | | | |
|---|---|---|---|
| ***Title:*** Assuring Effective Missions | 2.545 | 5.428 | 4.510 |

***Description:*** Develop the ability to assess and control the cyber situation within a military mission context. While the focus in cyber research is often placed on individual technologies, how these technologies work toward an effective mission is critical for the DoD. The objective of Assuring Effective Missions presents technology challenges in the areas of Cyber Mission Control and Effects at Scale. Cyber Mission Control covers the ability to orchestrate cyber systems to achieve an overarching mission goal. To perform dynamic analysis of asset criticality and course of action analysis alternatives, there is a critical need for tools that can map information technology assets to missions and use modeling and simulation, or other techniques. Inherent in Cyber Mission Control is the ability to automatically derive and fuse information about the characteristics of information technology systems in a manner that allows us to describe, analyze, observe, and control the operation of information technology components. A key goal of this research area is to have tools that enable commanders to assess and direct different information technology maneuvers in conjunction with mission actions. Effects at Scale encompass full spectrum challenges that intersect with cyber becoming a new full-fledged domain of warfare.

***FY 2014 Accomplishments:***

| B. Accomplishments/Planned Programs ($ in Millions) | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| - Automated mapping of mission essential functions to cyber resources using multi-attribute identifiers to enable commander's understanding of dependencies.<br>- Improved attack detection and graded response techniques to enhance survivability, attacker attribution, and adversarial deterrence.<br>- Enabled cyber effects assessment.<br>- Developed machine intelligence techniques for autonomous reprogramming, reconfiguration, and control of cyber components.<br>***FY 2015 Plans:***<br>- Develop metrics to support development and maintenance of Computer Network Defense (CND) capabilities to thwart certain classes of Advanced Persistent Threats (APT) and other threats.<br>- Create algorithms to identify and optimally configure critical cyber assets to assure effective missions.<br>- Assess effectiveness of agility mechanisms and moving target techniques against APT.<br>- Validate and extend machine intelligence techniques and theories based on experimental results.<br>- Develop agility metrics and evaluate within test environments to gauge the utility of agility maneuvers and validate ability to defend Offensive Cyber Operations (OCO) architecture.<br>***FY 2016 Plans:***<br>- Develop tools and techniques to assess and control the cyber situation in mission context.<br>- Develop cloud-based defense architecture system. | | | |
| ***Title:*** Cyber Modeling, Simulation & Experimentation (MSE)<br>***Description:*** Develop modeling and simulation capabilities that are able to sufficiently simulate the cyber environment in which the DoD operates and enable a more robust assessment and validation of cyber technology development. There are two technical challenges associated with cyber modeling, simulation, and experimentation: 1) Cyber Modeling and Simulation and 2) Cyber Measurement. Cyber Modeling and Simulation seeks to develop tools and techniques that enable analytical modeling and multi-scale simulation of complex cyber systems. Cyber Measurement develops cyber experimentation and test range technology to conduct controlled, repeatable experiments, providing the ability to track the progress of cyber research investments in a quantitative fashion. This area will explore new analytical methodologies, models, and experimental data sets to establish metrics to measure a system's state of security, apply the scientific method to establish the foundations of a framework in which cyber security research can be conducted, to test hypotheses with measurable and repeatable results, and the quantitative experimentation and assessment for new cyber technologies. These new methodologies will enable the exploration of modeling and simulation tools and techniques that can drive innovation in research. Additionally, these methodologies will aid in integrated experimentation by simulating the cyber environment with sufficient fidelity and integrating cyber modeling and simulation with the traditional modeling and simulation related to the kinetic domain.<br>***FY 2014 Accomplishments:*** | 0.850 | 2.262 | 2.036 |

| **B. Accomplishments/Planned Programs ($ in Millions)** | **FY 2014** | **FY 2015** | **FY 2016** |
|---|---|---|---|
| - Created a modeling and simulation (M&S) environment to support large scale cyberspace experiments and predictions that are currently not feasible with emulation/real information system test beds.<br>- Developed methods and tools to automate execution elements to support cyber experimentation.<br>***FY 2015 Plans:***<br>- Develop tools and techniques to automate situational awareness capabilities for large-scale mission-oriented experiments.<br>- Determine relevant metrics to measure progress and improvements that these tools will contribute to the state of art.<br>- Develop a selected set of vignettes and scenarios for combined cyberspace operations (cyber, Electronic-Warfare (EW), communications and network technologies), focusing on blue and red force interactions.<br>- Investigate application of causal workflows to combined cyberspace operations (cyber, EW, communications, and network technologies).<br>- Determine relevant test environments, design connectivity plan.<br>- Instrument primary test bed to support scenario generation and metric assessment.<br>***FY 2016 Plans:***<br>- Continue to develop a selected set of vignettes and scenarios for combined cyberspace operations (cyber, EW, communications, and network technologies) focusing on blue and red force interactions.<br>- Continue to investigate application of causal workflows to combined cyberspace operations (cyber, EW, communications, and network technologies).<br>- Continue to instrument primary test bed to support scenario generation and metric assessment/refinement.<br>- Investigate the dynamic nature of the system and how this can impact the metrics. | | | |
| ***Title:*** Embedded, Mobile & Tactical Environments (EMT)<br>***Description:*** Increase the focus of cyber S&T on DoD cyber systems that rely on technology beyond wired networking and standard computing platforms.  The objective in the area of embedded and tactical systems is to develop tools and techniques that assure the secure operation of microprocessors within our weapons platforms and systems; enable security in real-time systems; and establish security in disadvantaged, intermittent, and low-bandwidth environments.  This research also seeks to expand and cultivate military-grade techniques for securing and operating with enterprise-style commodity mobile devices, such as smartphones, tablets, and their associated infrastructures.  With the constant evolution of these devices and their respective infrastructures it is of the utmost importance to provide a secure environment where these devices can be effectively utilized, monitored and tracked.<br>***FY 2014 Accomplishments:***<br>- Developed efficient algorithms capable of locating and tracking stationary and mobile emitters to help protect DoD networks from wireless intrusion. | 0.622 | 4.694 | 4.798 |

| **Exhibit R-2A**, **RDT&E Project Justification:** PB 2016 Office of the Secretary Of Defense | | **Date:** February 2015 |
|---|---|---|
| **Appropriation/Budget Activity**<br>0400 / 2 | **R-1 Program Element (Number/Name)**<br>PE 0602668D8Z / *Cyber Security Research* | **Project (Number/Name)**<br>P003 / *Cyber Applied Research* |

## B. Accomplishments/Planned Programs ($ in Millions)

- Developed and tested hardware capable of rapidly providing accurate line of bearing to wireless emitters.

***FY 2015 Plans:***
- Design a robust common architecture that enables secure information sharing in a tactical environment.
- Develop approaches to detect counterfeit or malicious components in embedded hardware.
- Develop mission and threat scenario information, enumerating the threats to the avionics/platform of unmanned aerial systems (UAS).
- Inform Analysis of Alternatives for the UAS/ground control mission computer to include full avionics interface/systems.
- Complete pilot/operator cognitive task analyses.

***FY 2016 Plans:***
- Identify and characterize Advanced Persistent Threats (APT) to UAS platform avionics.
- Develop techniques to mitigate mission-deviant behavior directed by potential APT presence.
- Build and demonstrate situational awareness of the platform's cyber health to UAS pilots/operators and mission commanders.
- Develop prototype mission computer design suitable for application across a broad set of military and commercial/open bus architectures.

| | FY 2014 | FY 2015 | FY 2016 |
|---|---|---|---|
| **Accomplishments/Planned Programs Subtotals** | 11.637 | 14.979 | 13.727 |

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

| Line Item | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| • BA 3, PE # 0603668D8Z, P113: *Cyber Advanced Technology Development* | 11.150 | - | - | - | - | - | - | - | - | Continuing | Continuing |

**Remarks**

## D. Acquisition Strategy

N/A

## E. Performance Metrics

N/A