Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Office of the Secretary Of Defense	Date: February 2016
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*

COST ($ in Millions)	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
Total Program Element	-	17.748	13.701	12.183	-	12.183	15.043	15.323	15.535	15.840	Continuing	Continuing
P003: *Cyber Applied Research*	-	17.748	13.701	12.183	-	12.183	15.043	15.323	15.535	15.840	Continuing	Continuing

A. Mission Description and Budget Item Justification

Our military forces require resilient and reliable networks, computer systems, and embedded 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, along with protect tactical networks, weapons systems and platforms.

The Cyber Applied Research 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 (COI). New efforts will align with DoD Cyber Strategy and emerging U.S. Cyber Command (USCYBERCOM) mission requirements.

B. Program Change Summary ($ in Millions)	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Previous President's Budget	14.979	13.727	12.966	-	12.966
Current President's Budget	17.748	13.701	12.183	-	12.183
Total Adjustments	2.769	-0.026	-0.783	-	-0.783
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.411	-			
• Realignment for Higher Priority Programs	-	-	-0.689	-	-0.689
• FY15 Reprog. for Cancelled Account	-0.006	-	-	-	-
• Other Reprogrammings	3.186	-	-	-	-
• FFRDC Reduction	-	-0.026	-	-	-
• Economic Assumptions	-	-	-0.094	-	-0.094

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Office of the Secretary Of Defense	Date: February 2016
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602668D8Z *I Cyber Security Research*

Change Summary Explanation

FY 2017 internal realignment reflects funding for higher Departmental priorities and requirements.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense			Date: February 2016
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602668D8Z / *Cyber Security Research*	Project (Number/Name) P003 / *Cyber Applied Research*	

COST ($ in Millions)	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
P003: *Cyber Applied Research*	-	17.748	13.701	12.183	-	12.183	15.043	15.323	15.535	15.840	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 2015 Cyber Defense Strategy, Cyber Community of Interest (COI) 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 COI.

Beginning in FY 2013, the program expanded research in cyber command and control (C2) 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, efforts were aligned to U.S. Cyber Command (USCYBERCOM) mission assurance.

The six technical thrust areas of the Cyber Security Research Program 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 2015	FY 2016	FY 2017
Title: Foundations of Trust	1.742	1.425	1.270
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 2015 Accomplishments: This program funded the "Countermeasure to Commercial Off-The-Shelf Products" project, executed by the Air Force Research Laboratory (AFRL), to develop detection algorithms for malicious Universal Serial Bus (USB) firmware/hardware. A number of countermeasures were developed to mitigate hardware and firmware based attacks. This was demonstrated in a fully operational protection system that prevented, detected, and responded to supply chain attacks.			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
This program funded the Research Directorate of the National Security Agency (NSA) to develop a non-signature based capability to detect malicious code on cyber systems with high accuracy. This game changing approach to signature-free malware detection introduced a detection capability for defending against zero-day attacks. A new project initiated in FY 2015 focused research on Graphics Processing Unit (GPU) based image processing. During this fiscal year, this effort conducted experimentation and automated analytical techniques for the assessment of trustworthiness of DoD systems and components. Another new project funded in FY 2015 supported the tri-service execution of a five-eye international effort, under the Technical Cooperation Program's Cyber Strategic Challenge Group. This effort identified gaps in current vulnerability assessment tools in an effort to provide full coverage of the vulnerability landscape. These coverage gaps represent a demonstrated need for advanced cyber security tools. Through this program, the service laboratories will conduct research to develop/procure tools to address these gaps. ***FY 2016 Plans:*** This program will continue to fund the NSA to improve image processing computation by identifying and categorizing steps to improve GPU acceleration. This will help build a focused library of GPU tools. Another task will focus on building sets of advanced technique modules that will enhance capabilities of the meta-learning framework. ***FY 2017 Plans:*** Continuing efforts in FY 2017 will support developing approaches and methods to establish known degrees of assurance. Efforts this fiscal year will continue research to develop a system for combining many data structure extractors into one structure extractor (a process called "fusion"). Research will be conducted to continue furthering the capabilities of the meta-learning framework and expanding the library of GPU tools.			
Title: Resilient Infrastructure ***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. ***FY 2015 Accomplishments:***	2.720	0.940	0.950

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
This program funded the Naval Research Laboratory (NRL) and the Office of Naval Research (ONR) to address a number of critical gaps in Resilient Infrastructure. NRL executed a number of projects that improved the resiliency of tactical networks. The “Cross-Layer Resilient and Adaptive Networking" project enhanced the resilience of tactical wireless networking by using cross-layer principles to mitigate attacks through enhanced layer 1 agility. The use of cross-layer techniques helped influence higher layers which in turn helped identify advanced threats/attacks. The project developed methods for increasing resiliency of large scale tactical networks while enabling increased mobility. Development of the project offered technology transfer paths looking to increase model applicability to various types of ad-hoc and mesh networks. The other NRL executed projects, “Tactical Assured Information Sharing,” designed a framework for secure modularization and virtualization of nodes and networks. This high assurance software framework was highly configurable and executed trusted information flow. Software components were later implemented onto the Navy’s Network Pump-II security appliance, a cross domain solution (CDS). Under the newly funded FY 2015 “Tactical Platform Resiliency” project, ONR executed the development of cyber resiliency techniques and tools against attacks on known classes of cyber vulnerabilities. These vulnerabilities are applicable to Cyber Physical Systems (CPS) and, specifically, to hull, mechanical and electrical (HM&E) systems. The work has been assessed by a tri-service review board which addressed gaps in the protection of cyber physical systems controlling critical infrastructure. Through the modification and implementation of fault tolerant tools, a design has been developed that will effectively harden critical control systems from cyber disruption. Additionally a number of funded projects executed by Johns Hopkins University Applied Physics Laboratory (JHU/APL) and NRL addressed critical gaps in resilient infrastructure by maturing technologies through accelerated transition to operational partners. The first effort funded the “Control Flow Integrity Monitoring” project for transition to NSA, Department of Homeland Security (DHS), Defense Information Systems Agency (DISA), and the CERT Division of the Software Engineering Institute (SEI). This effort detected return-oriented programming attacks using record and replay technology. The technology enabled the rapid detection of zero-day attacks that bypass all modern defenses, eliminating the effectiveness of a large class of exploits. The second funded project executed by JHU/APL matured “System Cloaking Defense through Deception” technology to present decoys to adversaries and sense their presence and activities. A major impact of the project raised attacker workloads, confusing, delaying, and disrupting an adversary’s ability to execute exploitation operations. System Cloaking has been planned to transition to ONR, Army Cyber (ARCYBER), Marine Force Cyber (MARFORCYBER) and DHS. The last funded project was executed by NRL to mature and transition the “Network Pump-II.” Pump-II is a low-cost, high-throughput, government-off-the-shelf cross-domain solution. Transitions are planned to a number of programs of record, including the MQ-4C Triton unmanned aircraft			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
system (UAS) program, Navy's Program Executive Office Integrated Warfare Systems (PEO IWS) programs, and Air Force's Defense Cyber Program. ***FY 2016 Plans:*** A number of the funded projects will continue development through FY 2016, to include research executed under ONR for the "Tactical Platform Resiliency" project. ONR will improve the design and robustness of the variant fault tolerant tools used to harden critical control systems. The work will also design and develop capabilities to monitor and autonomously remove malicious code, commands and data from compromised networks, while preparing experimental frameworks for demonstration. The projects that have been designed to accelerate transition to operational partners will continue maturing capabilities, inhibiting advanced threats, improving Technology Readiness Level (TRL), and exploring transition opportunities. The involvement of committed customers in the transition process will accelerate maturation of the technology. Under the "Control Flow Integrity Monitoring" project, JHU/APL plans to increase the amount of information that it collects to drive improvements. Under the "System Cloaking" project, JHU/APL will work with ONR, ARCYBER, MARFORCYBER and DHS to tailor the product to customer needs. The NRL "Network Pump-II" project will work to improve on its TRL level, moving it closer to TRL 8. ***FY 2017 Plans:*** In FY 2017, ONR efforts under the "Tactical Platform Resiliency" project will develop methods and techniques for furnishing resiliency on critical real-time control systems against cyber-attacks. Additionally, ONR will work to experiment and evaluate resilience techniques through ONR Small Business Innovation Research (SBIR) performers. The projects that have been designed to accelerate transition to operational partners will continue maturing capabilities, inhibiting advanced threats, improving TRLs, and exploring transition opportunities.			
Title: Agile Operations ***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 Cyber Agility and Cyber Maneuver. Autonomic Cyber Agility covers several forms of agility for example, 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. 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 (repurposing a device or platform), reconfiguration (changing the way a system performs a task), and repositories (altering the operating state in a logical or physical topology). ***FY 2015 Accomplishments:*** This program funded the "Cyber Agility and Maneuver" project, executed by AFRL, to design distributed systems architectures and service application polymorphism. The work leveraged cyber agility, maneuver technology, and laboratory/experimentation	1.217	0.000	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
facilities to develop metrics and evaluate effectiveness against sophisticated attack types such as the Advanced Persistent Threat (APT). The project helped quantify metrics with which DoD could build, buy, configure, or maintain computer network defense (CND) capabilities to thwart certain classes of APTs and other classes of threats. Under the project AFRL collaborated with the Communications-Electronics Research, Development and Engineering Center (CERDEC) on their MORPHINATOR program with plans to share prototypes. In addition the work that was developed under "Cyber Agility and Maneuver" has been adopted into a Joint Service/Agency "Moving Target Defense (MTD) and Agility for Cyber Operations" collaboration working group. This in turn helped to develop automated reasoning techniques for executing courses of action, which was incorporated into the Air Force Rapid Acquisition Course of Action and Developmental Planning processes. ***FY 2016 Plans:*** Projects are concluding; the program is out briefing DoD stakeholders and transitioning efforts into relevant programs.			
Title: Assuring Effective Missions ***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 by developing tools and techniques that enable models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain. 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 2015 Accomplishments:*** This program funded projects executed by AFRL, CERDEC and NRL to address a number of gaps in Assured Effective Missions. AFRL's "Cyber Command & Control" project devised metrics to support development and maintenance of Computer Network Defense (CND) capabilities to thwart certain classes of APT. The effort created algorithms to identify and optimally configure critical cyber assets to assure effective missions. As a result, the Mission Assurance Framework developed under the project was applied to the Joint Space Operations Center (JSpOC) and the National Reconnaissance Office Operations Center (NROC). Another AFRL executed project, "Cyber Agility and Maneuver Characterization," assessed the effectiveness of agility mechanisms and moving target techniques against APTs. The work created real-world examples of mission and adversarial tasks that	6.015	4.476	3.675

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
culminated into a characterization of their benefits and limitations. The characterizations were then used to design a generic model/process to assess agile network defenses that measured moving target defense capabilities. NRL's "Situational Awareness through Network Science" project validated and extended machine intelligence techniques and theories for cyber application. Through the use of machine learning techniques, anomalous traffic patterns were identified to form an enhanced situational awareness picture to benefit network defenders. The program initiated a tri-service effort, led by CERDEC, called the "Defensible Offensive Cyber Operations (OCO) Architecture and Cyber Situational Awareness" project in FY 2015. FY 2015 efforts developed agility metrics and evaluated test environments to gauge the utility of agility maneuvers. The results were used to validate the ability to defend OCO architecture. Another tri-service program funded in FY 2015 supported the five-eye international effort, the Technical Cooperation Program's (TTCP) Cyber Strategic Challenge Group Project. This funding primarily augments existing S&T investments to make them interoperable with other nations TTCP contributions through the Canadian ARMOUR cyber framework to maximize potential leverage of TTCP investment. Additionally, this program funded the maturation of JHU/APL "Pointillist" capability. "Pointillist" provides easy-to-use rapid deployment Graphical User Interface configurations that support specialized use cases such as by the Cyber Protection hunt teams. This effort enables hunt teams to visualize graph data (for example network data flows) in real-time to rapidly identify and respond to adversaries. This effort was transitioned to MARFORCYBER. ***FY 2016 Plans:*** The "Defensible OCO Architecture and Cyber Situational Awareness" project will continue FY 2015 efforts and begin development of a cloud-based defense architecture system. ***FY 2017 Plans:*** During FY 2017, the "Defensible OCO Architecture and Cyber Situational Awareness" project will test the prototype cloud-based defense architecture. Upon successful completion of the testing, existing cyber situational awareness tools will be integrated and implemented into the OCO architecture.			
Title: Cyber Modeling, Simulation & Experimentation (MSE) ***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 MSE: 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	2.336	2.100	2.168

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
experiments, providing the ability to track the progress of cyber research investments in a quantitative fashion. This area explores 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. ***FY 2015 Accomplishments:*** This program initiated the "Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare and Communications/Networking" project executed by NRL. This project determined relevant metrics to enable the measurement of progress and improvements of tools utilized in this domain. The work developed a selected set of vignettes and scenarios of combined cyberspace operations that focused on blue/red force interactions. The vignettes offered a much more realistic evaluation of blue/red interactions and provided the DoD S&T community with a comprehensive and realistic environment for designing new cyber-EW systems. ***FY 2016 Plans:*** In FY 2016, the "Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare and Communications/ Networking" project will continue to develop the selected set of vignettes and scenarios for combined cyberspace operations that focus on blue and red force interactions. Additionally, the project will continue to instrument a primary test-bed in support of scenario generation and bolster metric assessment/refinement. ***FY 2017 Plans:*** During FY 2017, the "Metrics, Instrumentation and Emulation for Cyberspace Operations, Electronic Warfare and Communications/Networking" project will develop and fine-tune joint metrics that will be utilized in dynamic and causal workflows. Also, efforts will focus on validating real systems to ensure effective implementation.			
Title: Embedded, Mobile & Tactical Environments (EMT) ***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	3.718	4.760	4.120

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
infrastructures it is of the utmost importance to provide a secure environment where these devices can be effectively utilized, monitored and tracked. ***FY 2015 Accomplishments:*** During this fiscal year, this program initiated a tri-service project called "Resilient and Assured UAS Systems and Operations." This AFRL-led effort developed mission and threat scenario information that enumerated threats to the avionics/platform of unmanned aircraft systems (UAS). This protects mission data and reduces the risk of asset and data loss. The results of this first year's efforts informed an Analysis of Alternatives (AoA) for the UAS/ground control mission computer to include full avionics interface/systems. Additionally, this program funded a tri-service effort to support the international effort under the Technical Cooperation Program's Cyber Strategic Challenge Group Project. The effort developed exemplar concepts and capabilities across "EM Cyber" – those capabilities that exhibit an interdependence of electromagnetic and cyber technologies and which might link Cyber with other domains including Electronic Warfare (EW), Communications and Signals Intelligence (SIGINT). ***FY 2016 Plans:*** During this fiscal year, this program initiated a tri-service project called "Resilient and Assured UAS Systems and Operations." This AFRL-led effort developed mission and threat scenario information that enumerated threats to the avionics/platform of unmanned aircraft systems (UAS). This protects mission data and reduces the risk of asset and data loss. The results of this first year's efforts informed an Analysis of Alternatives (AoA) for the UAS/ground control mission computer to include full avionics interface/systems. Additionally, this program funded a tri-service effort to support the international effort under the Technical Cooperation Program's Cyber Strategic Challenge Group Project. The effort developed exemplar concepts and capabilities across "EM Cyber" – those capabilities that exhibit an interdependence of electromagnetic and cyber technologies and which might link Cyber with other domains including Electronic Warfare (EW), Communications and Signals Intelligence (SIGINT). ***FY 2017 Plans:*** Efforts during FY 2017 will demonstrate the prototype mission computer that integrates the capabilities developed in prior years. Potential transition opportunities to Air Force Life Cycle Management Center (AFLCMC), NRL, Naval Air Systems Command (NAVAIR), and CERDEC for experimentation.			
Accomplishments/Planned Programs Subtotals	17.748	13.701	12.183

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602668D8Z / *Cyber Security Research*	**Project (Number/Name)** P003 / *Cyber Applied Research*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A

THIS PAGE INTENTIONALLY LEFT BLANK