Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force											Date: May 2017	
Appropriation/Budget Activity 3600: *Research, Development, Test & Evaluation, Air Force* / BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*							
COST ($ in Millions)	**Prior Years**	**FY 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
Total Program Element	-	7.414	29.439	20.964	0.000	20.964	26.888	23.718	14.404	14.700	Continuing	Continuing
677820: *Computer Security RDTE: Firestarter*	-	5.797	5.555	6.491	0.000	6.491	6.355	6.472	6.585	6.721	Continuing	Continuing
677821: *Cyberspace Vulnerability Assessment*	-	0.143	22.378	13.176	0.000	13.176	18.956	15.634	6.179	6.306	Continuing	Continuing
677822: *Cyber Defense Analysis*	-	0.252	0.258	0.026	0.000	0.026	0.270	0.276	0.281	0.287	Continuing	Continuing
677823: *AFCERT*	-	1.222	1.248	1.271	0.000	1.271	1.307	1.336	1.359	1.386	Continuing	Continuing

A. Mission Description and Budget Item Justification

AF Defensive Cyberspace Operations (AF DCO) provides defensive cyber capabilities that protect the AFNET and DoD network enclaves, to include their associated computer systems, software applications and sensitive operational information against unauthorized intrusion, corruption, and/or destruction. The emphasis of the program is directed toward defensive cyberspace capabilities; computer and network systems security; damage assessment and recovery; cyber threat recognition, attribution, and mitigation; and active response methodologies in response to evolving threats and changes to cyber environment. These areas of emphasis are realized through research and development, test and acquisition in the areas of proactive defense, defensive counter cyberspace, cyberspace intelligence, surveillance and reconnaissance, command and control situational awareness, persistent network operations, as well as decision support, recovery, and digital forensics.

Firestarter utilizes cyber and Information Assurance (IA) technology investments by US Cyber Command, the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), Director of National Intelligence (DNI), Intelligence Advanced Research Projects Activity (IARPA), and the Department of Homeland Security (DHS), and various government research laboratories, to jump-start its development of solutions to existing Air Force cyber and IA requirements. This program supports AF Space Command's Cyberspace strategic direction in support of Cyber Defense which provides capabilities to 24th AF, as AF component to Cyber Command (CYBERCOM), Defense Information Systems Agency (DISA), National Security Agency (NSA), and other services to ensure Global Information Grid (GIG) cyber and IA requirements are being met. Activities performed include those designed to identify, analyze, test, rapidly acquire, and integrate emerging IA and cyber technology and defensive cyberspace weapons systems and capabilities into all regions of the GIG - terrestrial, airborne, and space systems. In addition, this effort will support implementation of DoD Enterprise-wide IA & Computer Network Defense (CND) Solutions Steering Group (ESSG) solutions. Current Air Force systems, such as the AFNET NIPRNet Gateways, SIPRNet Modernization program, and Host Based Security System leverage this technology to meet their information assurance and defensive cyberspace needs/requirements.

Cyberspace Vulnerability Assessment/ Hunter Team (CVA/H) weapon system develops new capabilities to provide Air Force Cyber Command (AFCYBER) and Combatant Commanders additional mobile precision in addition to currently fielded protection capabilities to identify, pursue, and mitigate cyberspace threats. The CVA/H weapon system performs defensive sorties world-wide via remote or on-site access. CVA/H executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The Hunter mission focuses on the capability to find, fix, track, target, engage, and assess (F2T2EA) the advanced

persistent threat (APT). This effort funds development efforts to enhance command and control situational awareness and to expand the capability of the current weapon system to meet scope and scale of the USCYBERCOM directed Cyber Protection Teams.

Cyberspace Defense Analysis (CDA) is an assessment of non-secure telecommunications to determine type and amount of sensitive and/or classified information that may have been disclosed to our adversaries and encompasses the following mission subsets: Telephony Communications, Radio Frequency (RF) Communications, E-mail Communications, Internet based Capabilities (IbC), Web Risk Assessment (WRA), and Cyber Operations Risk Assessment (CORA). CDA is the cyberspace weapon system that is used to conduct assessments during peace time and contingency operations. CDA shows its true capability in the force protection realm and helps ensure our adversaries are not provided early warning of our plans, capabilities, or limitations.

AF Computer Emergency Response Team (AFCERT) supports the AF Cyberspace Defense (ACD) weapon system and is designed to prevent, detect, and respond to adversarial penetration into AF unclassified and classified networks. ACD supports Air Force and Combatant Commanders by conducting synchronized Defensive Cyber Operations (DCO) and providing 24/7/365 monitoring and defense of USAF and US Central Command Secure/Non-secure Internet Protocol Router Network (SIPRNET/NIPRNET) systems against hostile attack. Daily intrusions to the AF network are analyzed in a forensics manner to identify a multitude of counter defensive and defensive tools and techniques that are required to truly strengthen cyber security. The Air Force Research Laboratory (AFRL) and other Federal R&D entities often have cutting edge solutions, that, with 3600 funding, can be taken to the technology readiness level (TRL) needed for rapid deployment as new capability to counter critical cyber weapon system vulnerabilities. AFCERT funding for this effort will focus on development of capability, capacity, and potential modifications to increase the utility of the ACD weapon system to the warfighter as well as testing requirements for new capabilities.

Activities include studies and analysis to support both current program planning and execution and future program planning.

These programs are in Budget Activity 7, Operational System Development, because this budget activity includes development efforts to upgrade systems that have been fielded or have received approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

B. Program Change Summary ($ in Millions)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	7.681	29.439	35.094	0.000	35.094
Current President's Budget	7.414	29.439	20.964	0.000	20.964
Total Adjustments	-0.267	0.000	-14.130	0.000	-14.130
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	0.000	0.000			
• SBIR/STTR Transfer	-0.267	0.000			
• Other Adjustments	0.000	0.000	-14.130	0.000	-14.130

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force	Date: May 2017
Appropriation/Budget Activity 3600: *Research, Development, Test & Evaluation, Air Force* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*

Change Summary Explanation

FY18 reduction of $14.130M for higher AF priorities.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677820 / *Computer Security RDTE: Firestarter*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
677820: *Computer Security RDTE: Firestarter*	-	5.797	5.555	6.491	0.000	6.491	6.355	6.472	6.585	6.721	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Firestarter program provides newly improved capabilities and technical transition opportunities for Cyber Defense and Information Assurance (IA) technologies and tools needed to defend Air Force Command, Control, Communications, Computer, and Intelligence (C4I) systems from Cyber-attacks, while ensuring recovery in the event of an attack. The emphasis of the program is directed toward defensive cyberspace capabilities; computer and network systems security; damage assessment and recovery; cyber threat recognition, attribution, and mitigation; and active response methodologies in response to evolving threats and changes to cyber environment. These areas of emphasis are realized through research and development, test and acquisition in the areas of proactive defense, defensive counter cyberspace, cyberspace intelligence, surveillance and reconnaissance & situational awareness, persistent network operations, as well as decision support, recovery, and digital forensics. Current Air Force systems, such as the AFNET NIPRNet Gateways, SIPRNet Modernization program, and Host Based Security System leverage this technology to meet their information assurance and defensive cyberspace needs/requirements.

Firestarter utilizes cyber and IA technology investments by US Cyber Command, the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), Director of National Intelligence (DNI), Intelligence Advanced Research Projects Activity (IARPA), and the Department of Homeland Security (DHS), and various government research laboratories, to jump-start its development of solutions to existing Air Force cyber and IA requirements. This program supports AF Space Command's Cyberspace strategic direction in support of Cyber Defense which provides capabilities to 24th AF, as AF component to Cyber Command (CYBERCOM), Defense Information Systems Agency (DISA), National Security Agency (NSA), and other services to ensure Global Information Grid (GIG) cyber and IA requirements are being met. Activities performed include those designed to identify, analyze, test, rapidly acquire, and integrate emerging IA and cyber technology and defensive cyberspace weapons systems and capabilities into all regions of the GIG - terrestrial, airborne, and space systems. In addition, this effort will support implementation of DoD Enterprise-wide Information Assurance (IA) & Computer Network Defense (CND) Solutions Steering Group (ESSG) solutions.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Cyber Forensic Tools & Methodologies	1.475	1.427	1.612
Description: Cyber forensic tools & methodologies. Includes initial metrics for reliable info assurance; secure coalition cyber data management, collaboration and visualization; analysis of cyber security bots			
FY 2016 Accomplishments: - Continued development of technologies to detect and attribute distributed computer network attacks over time and distance to specific adversaries			
FY 2017 Plans:			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
- Integrate memory forensics analysis techniques with real time network forensic capabilities and transition to appropriate Air Force cyber weapon systems ***FY 2018 Plans:*** - Will continue the development, enhancement, and transition of incident response data gathering and attack attribution technologies			
Title: Cyber Threat Recognition ***Description:*** Enhancing cyber platform technology to identify zero-day threats in real time. ***FY 2016 Accomplishments:*** - Continued development of technologies to detect and attribute distributed computer network attacks over time and distance to specific adversaries ***FY 2017 Plans:*** - Implement advanced techniques to correlate cyber intelligence data with real time network feeds to detect potential cyber intrusion and data exfiltration ***FY 2018 Plans:*** - Will normalize and automate methods and procedures to identify zero day cyber threats prior to system compromise	1.508	1.313	1.847
Title: Cyber Threat Attribution & Mitigation ***Description:*** Includes risk mitigation techniques for wireless networks and systems; active response, dynamic policy enforcement and computer/net attack attribution efforts. ***FY 2016 Accomplishments:*** - Continued development of technologies to detect and attribute distributed computer network attacks over time and distance to specific adversaries ***FY 2017 Plans:*** - Integrate technologies to detect and attribute distributed computer network attacks with appropriate USAF cyber weapon systems and pursue certification, accreditation, and authority to operate on USAF data networks ***FY 2018 Plans:*** - Will mature, enhance, and integrate developmental concepts to attribute cyber patterns, techniques, behaviors, and signatures to specific threat actors and identify mitigation strategies for each	1.615	1.710	1.733
Title: Transition of Cyber and Information Assurance Technologies	1.199	1.105	1.299

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Description: Transition cyber defense technologies that support AFSPC's Defense architecture. Includes space systems cyber solutions; terrestrial net defense technology development; airborne IP network cyber and IA tools; IA/cyber modeling & simulation; secure interoperable distributed agent computing, and others that relate to defending the AF networks. ***FY 2016 Accomplishments:*** - Enhanced and transitioned customer funded cyber and IA technology to operational USAF components in accordance with rapid requirements documentation provided by AFSPC ***FY 2017 Plans:*** - Continue enhancing and transitioning customer funded cyber and IA technology to operational USAF components in accordance with rapid requirements documentation provided by AFSPC ***FY 2018 Plans:*** - Will continue enhancing and transitioning customer funded cyber and IA technology to operational USAF components in accordance with rapid requirements documentation provided by AFSPC			
Accomplishments/Planned Programs Subtotals	5.797	5.555	6.491

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• N/A: *N/A*	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	-	-

Remarks

D. Acquisition Strategy

Firestarter conducts late stage Science and Technology (S&T) for tech demo and tech transition to warfighter employment. All contracts within this project are awarded using full and open competition and utilize evolutionary capability and incremental development. Where appropriate, collaborative efforts are conducted with services and agencies within the USAF to result in more robust and cost effective solutions. Contracting activities are primarily done through other agencies when deemed more advantageous. All aspects of the Firestarter project are managed by the Air Force Research Laboratory.

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677821 / *Cyberspace Vulnerability Assessment*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
677821: *Cyberspace Vulnerability Assessment*	-	0.143	22.378	13.176	0.000	13.176	18.956	15.634	6.179	6.306	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

In FY17, BA07 PE 0208088F, project 677821, Cyber Threat Mitigation, was a new start.
In FY17, BA07 PE 0208088F, project 677821, Defensive Next Generation Development, was a new start.

This requirement supports the Cyberspace Vulnerability Assessment / Hunter Team (CVA/H) weapon system development of new capabilities to provide Air Force Cyber Command (AFCYBER) and Combatant Commanders additional mobile precision in addition to currently fielded protection capabilities to identify, pursue, and mitigate cyberspace threats. The CVA/H weapon system performs defensive sorties world-wide via remote or on-site access. CVA/H executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The Hunter mission focuses on the capability to find, fix, track, target, engage, and assess(F2T2EA) the advanced persistent threat (APT). This effort funds development efforts to enhance command and control situational awareness and to expand the capability of the current weapon system to meet scope and scale of the USCYBERCOM directed Cyber Protection Teams.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Cyber Threat Mitigation	0.000	7.239	2.203
Description: Cyber Threat Mitigation includes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and supports Cyberspace Vulnerability Assessment/Hunter (CVH/H) missions in support of Air Force Cyber Command and Combatant Commanders.			
FY 2016 Accomplishments: N/A			
FY 2017 Plans: - Modernize CVA/H weapon system with emerging technologies to keep pace with an evolving cyber threat - Develop technologies to conduct vulnerability assessments, network intrusion analysis and systems vulnerability analysis (i.e, malware analysis capability, forensic analysis, visual analysis environment, distributed source code control vault and mission oriented mapping)			
FY 2018 Plans: - Will continue modernization of CVA/H weapon system with emerging technologies to keep pace with an evolving cyber threat			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
- Will continue development of technologies to conduct vulnerability assessments, network intrusion analysis and systems vulnerability analysis (i.e, malware analysis capability, forensic analysis, visual analysis environment, distributed source code control vault and mission oriented mapping)			
Title: Defensive Next Generation Development ***Description:*** Development of solutions supporting defensive cyber modernization and AF Cyber Needs Forms in the area of DCO capabilities and technologies to meet capability gaps required by Cyber Protection Teams. ***FY 2016 Accomplishments:*** N/A ***FY 2017 Plans:*** - Develop new solutions to support modernization of DCO capabilities and technologies to support Cyber Protection Teams (CPTs); includes multiple efforts (i.e., Data and Analysis and Traffic Inspection of SSL) ***FY 2018 Plans:*** Will deliver solutions to support modernization of DCO capabilities and technologies to support Cyber Protection Teams (CPTs); includes multiple efforts (i.e., Data and Analysis and Traffic Inspection of SSL)	0.000	14.719	9.973
Title: Test & Evaluation ***Description:*** Test and Evaluation provides both developmental testing of new development capabilities and a network environment for testing. ***FY 2016 Accomplishments:*** - Continued developmental testing support for new defensive capabilities and provided network environment for such testing ***FY 2017 Plans:*** - Continue developmental testing support for new defensive capabilities and provide for network environment for such testing ***FY 2018 Plans:*** - Will provide the required developmental testing for new platform, access, and capability products prior to fielding	0.143	0.420	1.000
Accomplishments/Planned Programs Subtotals	0.143	22.378	13.176

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF: BA03: Line Item # 831010: *COMSEC Equipment*	8.698	19.878	20.703	0.000	20.703	25.498	21.382	21.770	25.192	0.00	0.000

Remarks

D. Acquisition Strategy

The Cyberspace Vulnerability Assessment/Hunter (CVA/H) program office will utilize Concept, Development, Risk Management, or Production and Deployment Plans as part of a phased approach to acquisition planning. All plans will contain sufficient information for the Milestone Decision Authority (MDA) to determine readiness to enter into the applicable phase of the acquisition process. CVA/H Program office will utilize both new and existing contractual vehicles, in addition to existing Government-Wide Acquisition Contract (GWAC) vehicles (i.e, Alliant, Encore II, Solutions for Enterprise-Wide Procurement IV (SEWP IV), and General Services Administration (GSA) Federal Supply Schedules, Network-Centric Solutions (NETCENTs).

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Cyber Threat Mitigation-Malware Analysis	C/FFP	Various : Various	-	0.000		3.200	Jun 2017	0.000	Jun 2018	0.000		0.000	Continuing	Continuing	-
Cyber Threat Mitigation - Forensic Analysis	C/FFP	Various : Various	-	0.000		1.617	Jun 2017	0.000	Jun 2018	0.000		0.000	Continuing	Continuing	-
Cyber Threat Mitigation - Visual Analysis Enviroment	C/FFP	Various : Various	-	0.000		0.120	Mar 2017	0.000	Mar 2018	0.000		0.000	Continuing	Continuing	-
Cyber Threat Mitigation - Distributed Source Code Control Vault	C/FFP	Various : Various	-	0.000		0.177	May 2017	0.000	May 2018	0.000		0.000	Continuing	Continuing	-
Cyber Threat Mitigation - Mission Oriented Mapping	C/CPFF	Various : Various	-	0.000		2.125	Jan 2017	2.203	Jan 2018	0.000		2.203	Continuing	Continuing	-
Defensive Next Gen - Data & Analysis	C/CPFF	Various : Various	-	0.000		8.105	Mar 2017	2.143	Mar 2018	0.000		2.143	Continuing	Continuing	-
Defensive Next Gen - Training Simulator	C/FFP	Various : Various	-	0.000		5.440	Apr 2017	2.230	Apr 2018	0.000		2.230	Continuing	Continuing	-
Defensive Next Gen - Disc Forensics Solution	C/FFP	Various : Various	-	0.000		0.000		1.500	Mar 2018	0.000		1.500	Continuing	Continuing	-
Defensive Next Gen - Data Collection and Correlation	C/FFP	Various : Various	-	0.000		0.000		1.726	Mar 2018	0.000		1.726	Continuing	Continuing	-
Defensive Next Gen - Cloudshield Capabilities	C/FFP	Various : Various	-	0.000		0.000		1.200	Aug 2018	0.000		1.200	Continuing	Continuing	-
		Subtotal	-	0.000		20.784		11.002		0.000		11.002	-	-	-

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	-	-		-		-		-		-	-	-	-

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*	

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support	MIPR	46 Test Squadron : Eglin, FL	-	0.143		0.420	Oct 2016	1.000	Oct 2017	0.000		1.000	Continuing	Continuing	-
		Subtotal	-	0.143		0.420		1.000		0.000		1.000	-	-	-

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PMA - Engineering & Technical Asisstance Support Services (ETASS & FFRDC)	Various	AFLCMC/PZ : Bedford, MA	-	0.000	Jan 2016	1.174	Jan 2017	1.174	Jan 2018	0.000		1.174	Continuing	Continuing	-
		Subtotal	-	0.000		1.174		1.174		0.000		1.174	-	-	-

Remarks

Provides program engineering continuity, technical maturation and expertise, and access to an extensive professional network for future capabilities.

	Prior Years	FY 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	0.143		22.378		13.176		0.000		13.176	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

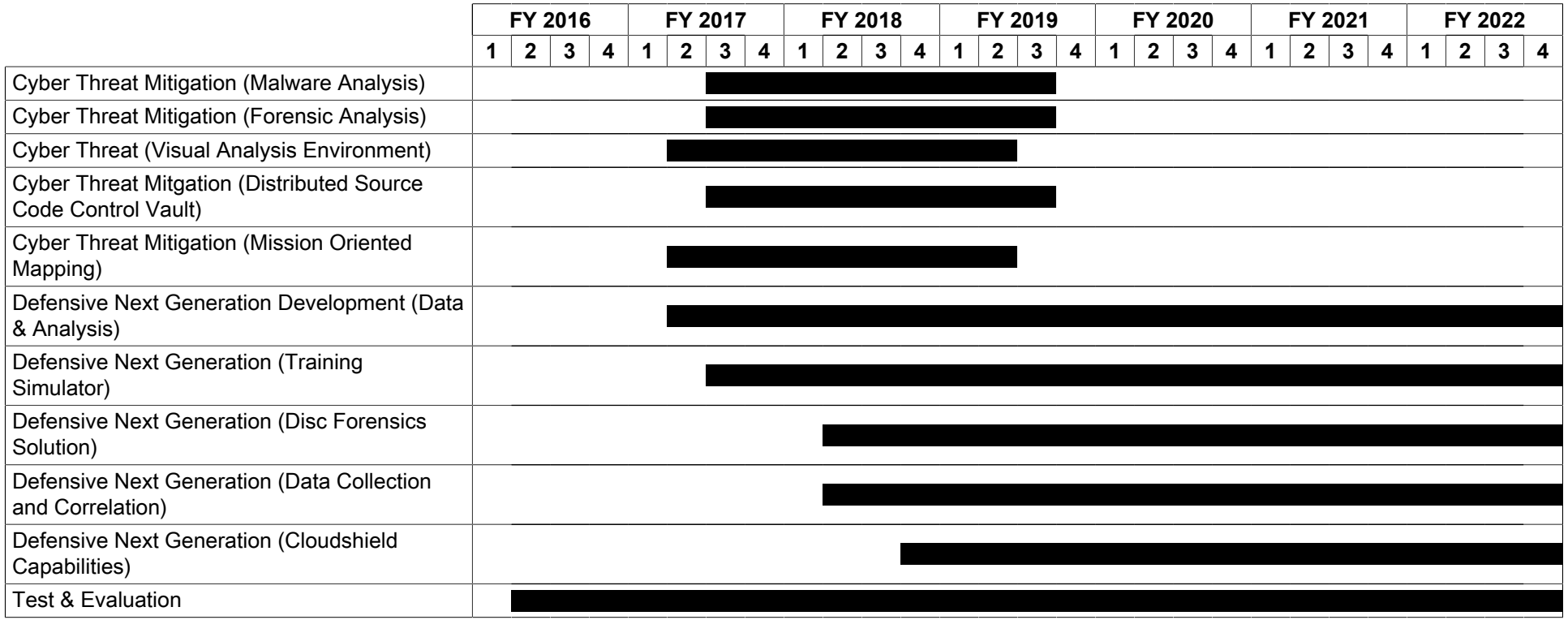

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Cyber Threat Mitigation (Malware Analysis)	3	2017	3	2019
Cyber Threat Mitigation (Forensic Analysis)	3	2017	3	2019
Cyber Threat (Visual Analysis Environment)	2	2017	2	2019
Cyber Threat Mitgation (Distributed Source Code Control Vault)	3	2017	3	2019
Cyber Threat Mitigation (Mission Oriented Mapping)	2	2017	2	2019
Defensive Next Generation Development (Data & Analysis)	2	2017	4	2022
Defensive Next Generation (Training Simulator)	3	2017	4	2022
Defensive Next Generation (Disc Forensics Solution)	2	2018	4	2022
Defensive Next Generation (Data Collection and Correlation)	2	2018	4	2022
Defensive Next Generation (Cloudshield Capabilities)	4	2018	4	2022
Test & Evaluation	2	2016	4	2022

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677822 / *Cyber Defense Analysis*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
677822: *Cyber Defense Analysis*	-	0.252	0.258	0.026	0.000	0.026	0.270	0.276	0.281	0.287	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Cyberspace Defense Analysis (CDA) is an assessment of non-secure telecommunications to determine type and amount of sensitive and/or classified information that may have been disclosed to our adversaries and encompasses the following mission subsets: Telephony Communications, Radio Frequency (RF) Communications, E-mail Communications, Internet based Capabilities (IbC), Web Risk Assessment (WRA), and Cyber Operations Risk Assessment (CORA). CDA is the cyberspace weapon system that is used to conduct assessments during peace time and contingency operations. CDA shows its true capability in the force protection realm and helps ensure our adversaries are not provided early warning of our plans, capabilities, or limitations.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Cyber Defense Analysis - Assessments	0.252	0.258	0.026
Description: Engineering support to conduct Cyberspace Defense Analysis (CDA) assessment of non-secure telecommunications during peace time and contingency operations. ***FY 2016 Accomplishments:*** - Supported CDA technical maturation and development of technologies to prevent disclosure of sensitive and/or classified information to adversaries ***FY 2017 Plans:*** - Continue support of CDA technical maturation and development of technologies to prevent disclosure of sensitive and/or classified information to adversaries that attempt to penetrate our networks ***FY 2018 Plans:*** - Will continue to support CDA technical maturation and development of technologies to prevent disclosure of sensitive and/or classified information to adversaries that attempt to penetrate our networks			
Accomplishments/Planned Programs Subtotals	0.252	0.258	0.026

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF: BA03: Line Item# 831010: *COMSEC Equipment*	2.136	0.244	3.940	0.000	3.940	1.268	1.279	1.284	7.349	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677822 / *Cyber Defense Analysis*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost

Remarks

D. Acquisition Strategy

The Cyberspace Defense Analysis (CDA) weapon system development of new capabilities to provide additional OPSEC protection capabilities to monitor, collect, analyze, and report cyberspace threats. The CDA program will utilize various contractual vehicles when necessary (i.e., Government-Wide Acquisition Contract (GWAC), Alliant, Encore II, Solutions for Enterprise-Wide Procurement IV (SEWP IV), and General Services Administration (GSA) Federal Supply Schedules, Network-Centric Solutions (NETCENTS) (mandatory for all IT services and supplies) and competitive contract (if required). The use of multiple-award contractual vehicles will provide a wide range of commercially-available products and services that should be able to meet requirements related to Defensive Cyberspace Operations.

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677823 / *AFCERT*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
677823: *AFCERT*	-	1.222	1.248	1.271	0.000	1.271	1.307	1.336	1.359	1.386	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

AF Computer Emergency Response Team (AFCERT) supports the AF Cyberspace Defense (ACD) weapons system and is designed to prevent, detect, and respond to adversarial penetration into AF unclassified and classified networks. ACD supports Air Force and Combatant Commanders by conducting synchronized Defensive Cyber Operations (DCO) and providing 24/7/365 monitoring and defense of USAF and US Central Command Secure/Non-secure Internet Protocol Router Network (SIPRNET/NIPRNET) systems against hostile attack. Daily intrusions to the AF network are analyzed in a forensics manner to identify a multitude of counter defensive and defensive tools and techniques that are required to truly strengthen cyber security. The Air Force Research Laboratory (AFRL) and other Federal R&D entities often have cutting edge solutions, that, with 3600 funding, take them to the technology readiness level (TRL) needed for rapid deployment as new capabilities to counter critical cyber weapon system vulnerabilities. AFCERT funding for this effort will focus on development of capability, capacity, and potential modifications to increase the utility of the ACD weapon system to the warfighter as well as testing requirements for new capabilities.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Cyberspace Defense Development	1.222	1.248	1.271
Description: Air Force Computer Emergency Response Team (AFCERT) prevention, detection, and response to adversarial penetration into AF unclassified and classified networks. ***FY 2016 Accomplishments:*** -Funding was not executed as part of the AFCERT BPAC 677823 for ACD requirements. Funding was reallocated to the FIRESTARTER BPAC 677820. ***FY 2017 Plans:*** -Funding was not executed as part of the AFCERT BPAC 677823 for ACD requirements. Funding was reallocated to the FIRESTARTER BPAC 677820. ***FY 2018 Plans:*** - Develop and test technologies for the AF Cyberspace Defensive (ACD) weapon system to prevent, detect, and respond adversarial penetration in AF networks			
Accomplishments/Planned Programs Subtotals	1.222	1.248	1.271

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677823 / *AFCERT*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF: BA03: Line Item # 831010: *COMSEC Equipment*	0.238	0.242	0.000	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
• OPAF: BA03: Line Item # 835080: *AFNET*	0.000	7.736	31.206	0.000	31.206	31.850	23.023	23.436	33.041	Continuing	Continuing

Remarks

D. Acquisition Strategy

The AF Cyberspace Defense (ACD) weapons system office will utilize existing contractual vehicles such as Massachusetts Institute of Technology Research and Engineering (MITRE), General Services Administration (GSA) Federal Supply Schedules, Air Force Research Laboratory (AFRL), Advisory and Assistance Services (A&AS) as well as various Test and Evaluation Enterprises. The ACD weapon system office also intends to utilize the commercial contracting community to lead the Development, Test and Integration of future Cyberspace Defense capabilities. The use of multiple-award contractual vehicles will provide a wide range of commercially-available products and services that should be able to meet many requirements related to the ACD mission.

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.