Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Air Force												Date: May 2021
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
Total Program Element	-	37.309	30.108	18.449	0.000	18.449	-	-	-	-	-	-
677820: *Computer Security RDTE: Firestarter*	-	24.413	21.467	8.527	0.000	8.527	-	-	-	-	-	-
677821: *Cyberspace Vulnerability Assessment*	-	11.350	7.015	8.288	0.000	8.288	-	-	-	-	-	-
677822: *Cyber Defense Analysis*	-	0.265	0.279	0.281	0.000	0.281	-	-	-	-	-	-
677823: *AFCERT*	-	1.281	1.347	1.353	0.000	1.353	-	-	-	-	-	-

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), 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 Cyberspace strategic direction in support of Cyber Defense which provides capabilities to 16th AF, as AF component to US Cyber Command (USCYBERCOM), 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 of AF and DoD networks and 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 the development efforts to enhance command and control situational awareness and to expand the capability of the current weapon system to meet the scope and scale of USCYBERCOM directed Cyber Protection Teams and AF Mission Defense 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 several mission subsets, including: Telephony Communications, Radio Frequency (RF) Communications, Email Communications, Internet based Capabilities (IbC), and Cyber Operations Risk Assessment (CORA). CDA is the cyberspace weapon system that is used to conduct assessments during peace time and contingency operations. The CDA weapon system protects the AF's critical information such as PII, OPSEC, and other sensitive information through passive monitoring and active Data Loss Protection (DLP). 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. Continued funding is essential in developing new capabilities to combat the rapidly evolving cyber threat.

Cyberspace Defense Analysis (CDA): The CDA weapon system conducts Defensive Cyberspace Operations (DCO) and network defense by monitoring, collecting, analyzing, and reporting sensitive information transiting or residing on the AFNet. Without proper funding the CDA Operators will not be able to determine potential impacts and operational adjustments resulting from information disclosures or identify compromised information from network intrusions. There will be a decreased assurance of network defense and an increase in the amount of lost PII, OPSEC, and other sensitive information. The CDA mission subsets include: Telephony Communications, Radio Frequency (RF) Communications, Email Communications, Internet based Capabilities (IbC), 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, OPSEC, Data Loss Prevention, etc. and helps ensure our adversaries are not provided early warning of our plans, capabilities, or limitations. Continuing funding is essential in developing new capabilities to combat the rapidly evolving cyber threats.

The Cyberspace Defense Analysis (CDA) weapon system must development new capabilities to provide additional information protection capabilities to monitor, collect, analyze, and report cyberspace threats and identify compromised data. These capabilities encompass the support to OPSEC protection and Data Loss Prevention. The CDA program will utilize various contractual vehicles when necessary such as Solutions for Enterprise-Wide Procurement IV (SEWP IV), General Services Administration (GSA) Federal Supply Schedules, Network-Centric Solutions (NETCENTS), and other competitive contracts (if required). The use of multiple-award contractual vehicles provide access to a wide range of commercially-available products and services required to meet Defensive Cyber Operations requirements related to combat the rapidly evolving cyber threats.

The AF Cyberspace Defense (ACD) weapon system 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), Air Force CyberWorx and other Federal R&D entities often have cutting edge solutions, that, with Research and Development funding, can be taken to the technology readiness level (TRL) needed for rapid deployment as new capability to counter critical cyber weapon system vulnerabilities. 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Air Force	Date: May 2021
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*

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

This program element may include necessary civilian pay expenses required to manage, execute, and deliver weapon system capability. The use of such programs funds would be in addition to the civilian pay expenses budgeted in program element 0605831F. In FY20 $0.075M was expended for civilian pay expenses in this program element, and in FY21 $0.103M is forecasted for civilian pay expenses in this program element.

This program is 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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	38.609	15.165	18.726	0.000	18.726
Current President's Budget	37.309	30.108	18.449	0.000	18.449
Total Adjustments	-1.300	14.943	-0.277	0.000	-0.277
• Congressional General Reductions	0.000	-0.055			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	15.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	0.000	0.000			
• SBIR/STTR Transfer	-1.300	0.000			
• Other Adjustments	0.000	-0.002	-0.277	0.000	-0.277

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2020	FY 2021
Project: 677820: *Computer Security RDTE: Firestarter*		
Congressional Add: *Critical Infrastructure Cyber Security*	10.000	15.000
Congressional Add: *Cyber Resilient Space Architecture*	12.000	-
Congressional Add Subtotals for Project: 677820	22.000	15.000
Congressional Add Totals for all Projects	22.000	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
677820: *Computer Security RDTE: Firestarter*	-	24.413	21.467	8.527	0.000	8.527	-	-	-	-	-	-
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 Cyberspace strategic direction in support of Cyber Defense which provides capabilities to 16th AF, as AF component to US Cyber Command (USCYBERCOM), 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.

This program element may include necessary emergent or unanticipated civilian pay expenses required to manage, execute, and deliver Firestarter for emergent or unanticipated weapon system capabilities. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyber Forensic Tools & Methodologies	0.512	1.400	-
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 2021 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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 2020	FY 2021	FY 2022
- Continue the development, enhancement, and transition of incident response data gathering and attack attribution technologies ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding decreased due to consolidation of activities into Transition of Cyber Information Assurance Technologies to more accurately represent program efforts.			
Title: Cyber Threat Recognition ***Description:*** Enhancing cyber platform technology to identify zero-day threats in real time. ***FY 2021 Plans:*** - Continue to normalize and automate methods and procedures to identify zero day cyber threats prior to system compromise ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding decreased due to consolidation of activities into Transition of Cyber Information Assurance Technologies to more accurately represent program efforts.	0.526	1.599	-
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 2021 Plans:*** - Continue to mature, enhance, and integrate developmental concepts to attribute cyber patterns, techniques, behaviors, and signatures to specific threat actors and identify mitigation strategies for each ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding decreased due to consolidation of activities into Transition of Cyber Information Assurance Technologies to more accurately represent program efforts.	0.500	0.815	-
Title: Transition of Cyber and Information Assurance Technologies ***Description:*** Transition of advanced cyber defense technologies that support AF Defensive Cyber Operations 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 2021 Plans:***	0.875	2.653	8.527

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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 2020	FY 2021	FY 2022
- Continue enhancing and transitioning customer funded cyber and IA technology to operational USAF components in accordance with rapid requirements documentation ***FY 2022 Plans:*** - Will continue enhancing and transitioning customer funded cyber and IA technology to operational USAF components in accordance with rapid requirements documentation ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding increased due to consolidation of activities to more accurately represent program efforts.			
Accomplishments/Planned Programs Subtotals	2.413	6.467	8.527

	FY 2020	FY 2021
Congressional Add: Critical Infrastructure Cyber Security ***FY 2020 Accomplishments:*** - Craft and execute Critical Infrastructure Cyber Security research and development plan - Perform research; develop test plans, exercises, and security configurations; conduct assessments; and complete technical reports on a variety of Air Force critical infrastructure and interfaces ***FY 2021 Plans:*** - Continue to craft and execute Critical Infrastructure Cyber Security research and development plan - Continue to perform research; develop test plans, exercises, and security configurations; conduct assessments; and complete technical reports on a variety of Air Force critical infrastructure and interfaces	10.000	15.000
Congressional Add: Cyber Resilient Space Architecture ***FY 2020 Accomplishments:*** - Craft and execute cyber resilient space architecture research and development plan - Perform research; develop security profiles, integrate developmental concepts and enhance security configurations; conduct assessments; and complete technical reports on a variety of space system architectures - Transition cyber technologies for use in space enterprise	12.000	-
Congressional Adds Subtotals	22.000	15.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Beginning in FY22, planned programs realigned to Transition of Cyber and Information Assurance Technologies in order to more accurately represent planned activities.

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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force		Date: May 2021
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*

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Firestarter Development	C/CPFF	Various : Various	-	22.859	Jan 2020	18.370	Jan 2021	4.511	Jan 2022	-		4.511	-	-	-
Firestarter Integration	C/CPFF	Various : Various	-	0.638	Jan 2020	1.499	Jan 2021	1.929	Jan 2022	-		1.929	-	-	-
		Subtotal	-	23.497		19.869		6.440		-		6.440	-	-	N/A

Remarks

Multiple contractors and multiple universities reflect on-going efforts with over a dozen contractors and universities. Each has a different contract date depending on when that particular contract was awarded.

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Firestarter Testing	C/CPFF	Various : Various	-	0.691	Jan 2020	1.373	Jan 2021	1.862	Jan 2022	-		1.862	-	-	-
		Subtotal	-	0.691		1.373		1.862		-		1.862	-	-	N/A

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Firestarter PMA	C/CPFF	Various : Various	-	0.225	Jan 2020	0.225	Jan 2021	0.225	Jan 2022	-		0.225	-	-	-
		Subtotal	-	0.225		0.225		0.225		-		0.225	-	-	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	24.413		21.467		8.527		-		8.527	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Air Force		Date: May 2021
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*

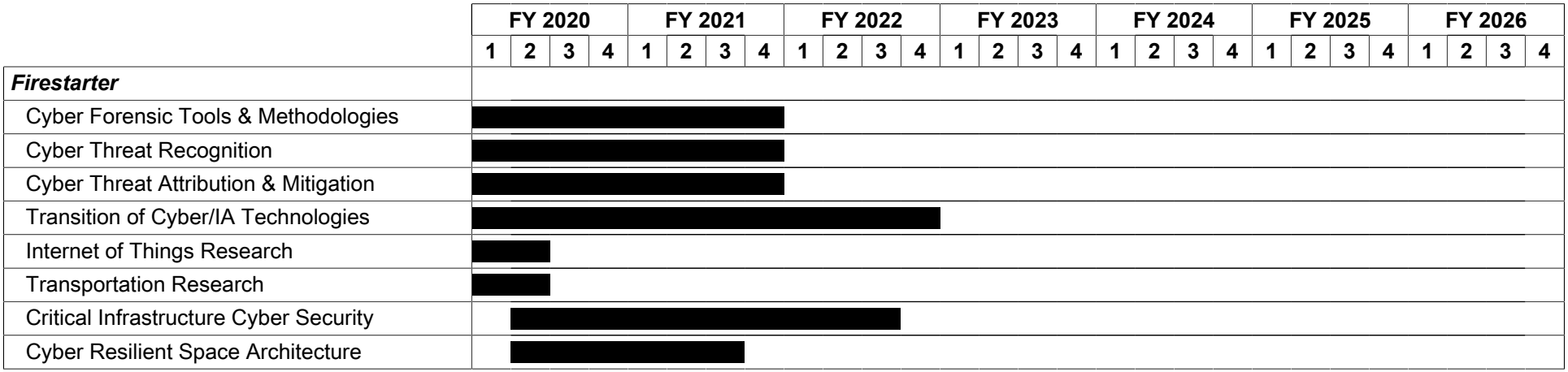

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Firestarter				
Cyber Forensic Tools & Methodologies	1	2020	4	2021
Cyber Threat Recognition	1	2020	4	2021
Cyber Threat Attribution & Mitigation	1	2020	4	2021
Transition of Cyber/IA Technologies	1	2020	4	2022
Internet of Things Research	1	2020	2	2020
Transportation Research	1	2020	2	2020
Critical Infrastructure Cyber Security	2	2020	3	2022
Cyber Resilient Space Architecture	2	2020	3	2021

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
677821: *Cyberspace Vulnerability Assessment*	-	11.350	7.015	8.288	0.000	8.288	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

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 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 and AF Mission Defense Teams.

This program element may include necessary emergent or unanticipated civilian pay expenses required to manage, execute, and deliver Cyberspace Vulnerability Assessment/Hunter for emergent or unanticipated weapon system capabilities. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605829F. In FY2020(PY) 0.075M was expended for civilian pay expenses in this program element.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyber Threat Mitigation	0.800	0.400	0.718
Description: Cyber Threat Mitigation includes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and supports Cyberspace Vulnerability Assessment/Hunter (CVA/H) missions in support of Air Force Cyber Command and Combatant Commanders.			
FY 2021 Plans: Continue development and integration of technologies to conduct vulnerability assessments, network intrusion analysis and systems vulnerability analysis			
FY 2022 Plans: Will continue development and integration of technologies to conduct vulnerability assessments, network intrusion analysis and systems vulnerability analysis			
FY 2021 to FY 2022 Increase/Decrease Statement:			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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 2020	FY 2021	FY 2022
Funding increased due to additional cyber threat recognition requirements.			
Title: Defensive Next Generation Development ***Description:*** Development and integration 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 and Mission Defense Teams. ***FY 2021 Plans:*** Continue development and integration to support modernization of DCO capabilities and technologies to support Cyber Protection Teams and Mission Defense Teams ***FY 2022 Plans:*** Will continue development and integration to support modernization of DCO capabilities and technologies to support Cyber Protection Teams and Mission Defense Teams ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding Increase due to additional support requirements for Cyber CPT and MDT Priorities	9.550	5.615	6.570
Title: Test & Evaluation Description: Test and Evaluation ***Description:*** Test and Evaluation provides both developmental testing of new capabilities and the test environments for validating the capabilities. ***FY 2021 Plans:*** Continue development testing for DCO capability products and technologies prior to fielding ***FY 2022 Plans:*** Will continue development testing for DCO capability products and technologies prior to fielding ***FY 2021 to FY 2022 Increase/Decrease Statement:*** N/A	1.000	1.000	1.000
Accomplishments/Planned Programs Subtotals	11.350	7.015	8.288

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• OPAF 03 831010: *Comsec Equipment*	12.654	-	-	-	-	-	-	-	-	-	-
• OPAF 03 834320: *C3 Countermeasures*	-	22.616	27.770	-	27.770	-	-	-	-	-	-

Remarks

Beginning in FY21 associated OPAF realigned from COMSEC Equipment WSC to C3 Countermeasures WSC for clarity in reporting.

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 such as Alliant, Encore II, Solutions for Enterprise-Wide Procurement IV (SEWP IV), and General Services Administration (GSA) Federal Supply Schedules, Network-Centric Solutions (NETCENTs).

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force			Date: May 2021
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 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Cyber Threat Mitigation - Threat Intelligence	C/CPFF	Various : Various	-	0.800	Jan 2020	0.400	Jan 2021	0.680	Jan 2022	-		0.680	-	-	-
Defensive Next Gen - Data & Analysis	C/CPFF	Various : Various	-	0.850	Mar 2020	0.716	Mar 2021	0.800	Mar 2022	-		0.800	-	-	-
Defensive Next Gen - Sensor Optimization	C/FFP	Various : Various	-	2.649	May 2020	1.105	May 2021	1.100	May 2022	-		1.100	-	-	-
Defensive Next Gen - Training Simulator	C/FFP	Various : Various	-	2.550	Apr 2020	0.670	Apr 2021	1.440	Apr 2022	-		1.440	-	-	-
Defensive Next Gen - Data Collection and Correlation	C/FFP	Various : Various	-	1.031	Mar 2020	0.666	Mar 2021	0.648	Mar 2022	-		0.648	-	-	-
Defensive Next Gen - Intrusion Prevention Capabilities	C/FFP	Various : Various	-	0.690	Aug 2020	0.656	Aug 2021	0.700	Aug 2022	-		0.700	-	-	-
		Subtotal	-	8.570		4.213		5.368		-		5.368	-	-	N/A

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Direct Cite Authority Civilian Pay	TBD	USAF : Hanscom AFB, MA	-	0.075	Oct 2019	0.103	Oct 2020	0.228	Oct 2021	-		0.228	-	-	-
		Subtotal	-	0.075		0.103		0.228		-		0.228	-	-	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support	MIPR	46 Test Squadron : Eglin, FL	-	1.000	Oct 2019	1.000	Oct 2020	1.000	Oct 2021	-		1.000	-	-	-
		Subtotal	-	1.000		1.000		1.000		-		1.000	-	-	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force			Date: May 2021
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677821 / *Cyberspace Vulnerability Assessment*	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PMA - Engineering & Technical Asisstance Support Services (ETASS & FFRDC)	Various	AFLCMC/PZ : Bedford, MA	-	1.705	Jan 2020	1.699	Jan 2021	1.692	Jan 2022	-		1.692	-	-	-
		Subtotal	-	1.705		1.699		1.692		-		1.692	-	-	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	11.350		7.015		8.288		-		8.288	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

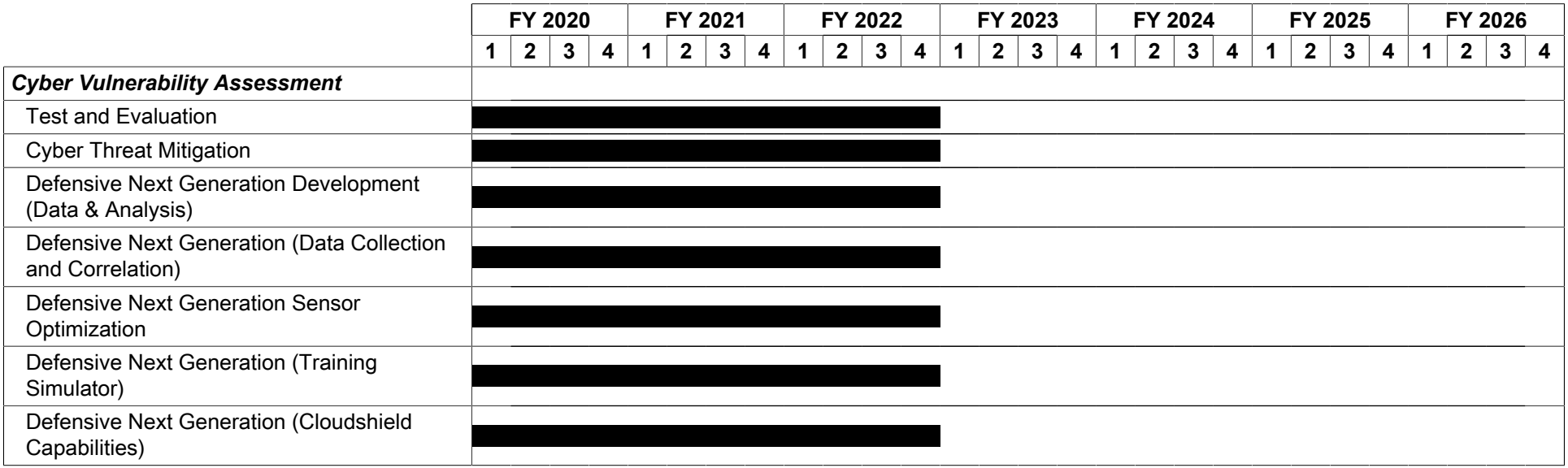

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677821 / *Cyberspace Vulnerability Assessment*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Cyber Vulnerability Assessment				
Test and Evaluation	1	2020	4	2022
Cyber Threat Mitigation	1	2020	4	2022
Defensive Next Generation Development (Data & Analysis)	1	2020	4	2022
Defensive Next Generation (Data Collection and Correlation)	1	2020	4	2022
Defensive Next Generation Sensor Optimization	1	2020	4	2022
Defensive Next Generation (Training Simulator)	1	2020	4	2022
Defensive Next Generation (Cloudshield Capabilities)	1	2020	4	2022

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
677822: *Cyber Defense Analysis*	-	0.265	0.279	0.281	0.000	0.281	-	-	-	-	-	-
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 several mission subsets, including: Telephony Communications, Radio Frequency (RF) Communications, Email Communications, Internet based Capabilities (IbC), and Cyber Operations Risk Assessment (CORA). CDA is the cyberspace weapon system that is used to conduct assessments during peace time and contingency operations. The CDA weapon system protects the AF's critical information such as PII, OPSEC, and other sensitive information through passive monitoring and active Data Loss Protection (DLP). 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. Continued funding is essential in developing new capabilities to combat the rapidly evolving cyber threat.

Cyberspace Defense Analysis (CDA): The CDA weapon system conducts Defensive Cyberspace Operations (DCO) and network defense by monitoring, collecting, analyzing, and reporting sensitive information transiting or residing on the AFNet. Without proper funding the CDA Operators will not be able to determine potential impacts and operational adjustments resulting from information disclosures or identify compromised information from network intrusions. There will be a decreased assurance of network defense and an increase in the amount of lost PII, OPSEC, and other sensitive information. The CDA mission subsets include: Telephony Communications, Radio Frequency (RF) Communications, Email Communications, Internet based Capabilities (IbC), 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, OPSEC, Data Loss Prevention, etc. and helps ensure our adversaries are not provided early warning of our plans, capabilities, or limitations. Continuing funding is essential in developing new capabilities to combat the rapidly evolving cyber threats.

The Cyberspace Defense Analysis (CDA) weapon system must development new capabilities to provide additional information protection capabilities to monitor, collect, analyze, and report cyberspace threats and identify compromised data. These capabilities encompass the support to OPSEC protection and Data Loss Prevention. The CDA program will utilize various contractual vehicles when necessary such as Solutions for Enterprise-Wide Procurement IV (SEWP IV), General Services Administration (GSA) Federal Supply Schedules, Network-Centric Solutions (NETCENTS), and other competitive contracts (if required). The use of multiple-award contractual vehicles provide access to a wide range of commercially-available products and services required to meet Defensive Cyber Operations requirements related to combat the rapidly evolving cyber threats.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyber Defense Analysis	0.265	0.279	0.281
Description: Engineering support to conduct Cyberspace Defense Analysis (CDA) assessment of non-secure telecommunications during peace time and contingency operations.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677822 / *Cyber Defense Analysis*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
FY 2021 Plans: Continue support of development of data loss prevention technologies and support to insider threat detection capabilities. Support technology areas that prevent adversaries' attempts to get into our networks. ***FY 2022 Plans:*** Will continue support of development of data loss prevention technologies and support to insider threat detection capabilities. Support technology areas that prevent adversaries' attempts to get into our networks. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding increased due to inflation adjustment			
Accomplishments/Planned Programs Subtotals	0.265	0.279	0.281

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• OPAF 03 Line Item 831010: *COMSEC Equipment*	1.698	-	-	-	-	-	-	-	-	-	-
• OPAF 03 834320: *C3 Countermeasures*	-	1.699	10.374	-	10.374	-	-	-	-	-	-

Remarks

Beginning in FY21 associated OPAF realigned from COMSEC Equipment WSC 831010 to C3 Countermeasures WSC 834320 for clarity in reporting.

D. Acquisition Strategy

The Cyberspace Defense Analysis (CDA) Weapon System development of new capabilities to provide additional information protection capabilities to monitor, collect, analyze, and report cyberspace threats and compromised data. These capabilities encompass the support to OPSEC protection as well. The CDA program will utilize various contractual vehicles when necessary such as 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) 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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force			Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677822 / *Cyber Defense Analysis*	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
CDA PMA - Engineering & Technical Assistance Support Services (ETASS & FFRDC)	Various	AFLCMC/PZ : Hanscom, MA	-	0.265	Jan 2020	0.279	Jan 2021	0.281	Jan 2022	-		0.281	-	-	-
		Subtotal	-	0.265		0.279		0.281		-		0.281	-	-	N/A

Remarks

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

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	0.265		0.279		0.281		-		0.281	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677822 / *Cyber Defense Analysis*

	FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025				FY 2026			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Cyber Defense Analysis																												
Cyber Defense Analysis (FFRDC)	[redacted]																											

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677822 / *Cyber Defense Analysis*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Cyber Defense Analysis				
Cyber Defense Analysis (FFRDC)	1	2020	4	2022

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
677823: *AFCERT*	-	1.281	1.347	1.353	0.000	1.353	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The AF Cyberspace Defense (ACD) weapon system 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), Air Force CyberWorx, and other Federal R&D entities often have cutting edge solutions, that, with Research and Development 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.

This program element may include necessary emergent or unanticipated civilian pay expenses required to manage, execute, and deliver AF Cyberspace Defense for emergent or unanticipated weapon system capabilities. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyberspace Defense Development	1.281	1.347	1.353
Description: AF Cyberspace Defense (ACD) weapon system to prevent, detect, and respond to adversarial penetration in AF networks			
FY 2021 Plans: - Develop and test technologies for the AF Cyberspace Defense (ACD) weapon system to prevent, detect, and respond to adversarial penetration in AF networks			
FY 2022 Plans: - Will continue to develop and test technologies for the AF Cyberspace Defense (ACD) weapon system to prevent, detect, and respond to adversarial penetration in AF networks			
FY 2021 to FY 2022 Increase/Decrease Statement: N/A			
Accomplishments/Planned Programs Subtotals	1.281	1.347	1.353

Exhibit R-2A, RDT&E Project Justification: PB 2022 Air Force		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• OPAF 03 Line Item 835080: *AFNET*	16.883	-	-	-	-	-	-	-	-	-	-
• OPAF 03 834320: *C3 Countermeasures*	-	23.860	35.463	-	35.463	-	-	-	-	-	-

Remarks

Beginning in FY21 associated OPAF realigned from AFNET WSC 835080 to C3 Countermeasures WSC 834320 for clarity in reporting.

D. Acquisition Strategy

The AF Cyberspace Defense (ACD) weapon 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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Air Force			Date: May 2021
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0208088F / *AF Defensive Cyberspace Operations*	Project (Number/Name) 677823 / *AFCERT*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
ACD Cyberspace Defense Development	C/CPAF	Various : Various	-	1.281	Aug 2020	1.347	Oct 2020	1.353	Oct 2021	-		1.353	-	-	-
		Subtotal	-	1.281		1.347		1.353		-		1.353	-	-	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	1.281		1.347		1.353		-		1.353	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677823 / *AFCERT*

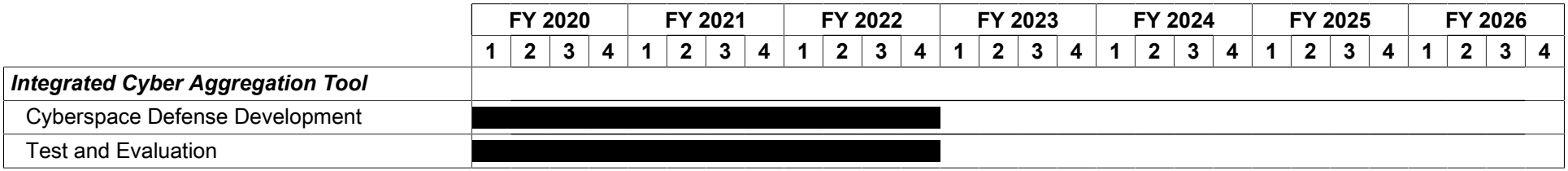

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Air Force		Date: May 2021
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0208088F / *AF Defensive Cyberspace Operations*	**Project (Number/Name)** 677823 / *AFCERT*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Integrated Cyber Aggregation Tool				
Cyberspace Defense Development	1	2020	4	2022
Test and Evaluation	1	2020	4	2022