Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Army	**Date:** March 2019
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 5: *System Development & Demonstration (SDD)*	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	41.441	33.796	62.262	-	62.262	29.738	92.873	94.974	90.000	0.000	445.084
CY5: *CYBER Situational Understanding*	-	0.000	0.000	20.183	-	20.183	0.000	0.000	0.000	0.000	0.000	20.183
EV5: *Defensive CYBER Operations*	-	41.441	33.796	42.079	-	42.079	29.738	92.873	94.974	90.000	0.000	424.901

Note

Project CY5 is a new start beginning in FY20.

A. Mission Description and Budget Item Justification

Defensive Cyber Tool Development (DCTD) and Cyber Situational Understanding (SU) fall within Line of Effort (LOE) 1 of the Network Modernization Strategy framework, which incorporates cyber capabilities that support the employment of the network as a weapon system.

Overall, Defensive Cyber Operations (DCO) and Cyber SU provide the tools and insight to proactively protect and defend the network at the tactical and strategic levels, thereby enabling the network to operate unfettered from the threat of cyberattacks.

CY5 Cyber SU:

Cyber SU supports Cyber Electromagnetic Activity (CEMA) operations by providing visualization of CEMA information to improve planning, coordination, integration and synchronization of cyberspace operations and unified land operations.

Cyber SU provides the Brigade to Corps commanders the visualization of physical (geographically), logical (at a specific network internet protocol), and cyber persona layers (bad actors, from individuals to nation states) of cyberspace based on data/information from multiple sources and sensors to produce a CEMA overlay on the commander's Common Operational Picture (COP) within the Command Post Computing Environment (CPCE). Supporting CEMA, Cyber SU synchronizes and integrates red (enemy), grey (commercial/private sector) and blue (friendly) cyberspace data, and enables collaboration at the tactical echelon. Further, in support of the Military Decision Making Process (planning and decision cycles), Cyber SU provides tactical commanders with a broad understanding of CEMA threats by informing the commander of any cyber related impacts to physical domains, unified land operations, and the overall mission.

EV5 DCO:

The DCO group of programs develops, assesses, deploys, learns, and iterates essential cyberspace warfighting capabilities consisting of solutions based upon an infrastructure, platform, and tool/payload approach. DCO capabilities are required in order to actively predict and conduct reconnaissance (search and discover) against advanced cyberspace threats (to include insider threats) and vulnerabilities that do not trigger or generate warnings using routine security measures. Additionally,

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Army	**Date:** March 2019
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 5: *System Development & Demonstration (SDD)*	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*

DCO capabilities allow the Army to outmaneuver adversaries by performing preapproved, automated, agile, internal countermeasures that stop or mitigate cyberspace attacks. Moreover, DCO capabilities enable the Army to conduct cyberspace defense mission planning and protection that identifies and assures the availability of tasked critical assets and infrastructure supporting Army, DOD, host nation, and civil authority actions or missions. The overall objective is to achieve survivability of networks, IT platforms, and data through counter-mobility actions, dynamic movement of tasked critical assets, and security enhancement measures. This assures commanders from U.S. Army Cyber Command (ARCYBER) and other Army Service Component Commands Brigade through Corp down to the tactical level can execute national, joint, and/or Army operational and tactical missions. These capabilities enable ARCYBER to support U.S. Cyber Command (USCYBERCOM) and defend all Army networks as part of its Service-retained responsibilities. DCO capabilities also enable Army National Guard and Reserve forces to support USC Title 10 missions under the auspices of ARCYBER or other major commands.

DCO supports material solutions aligned to requirements outlined in the 26 October 2016 Joint Requirements Oversight Council (JROC) Defensive Cyberspace Operations Information Systems Initial Capabilities Document (IS ICD). DCO related infrastructure, platforms, and tools/payloads enable the Army to maneuver, conduct reconnaissance, execute counter-mobility actions, and command and control DCO people, processes, and technologies within friendly cyberspace. DCO programs will allow near real-time employment of passive and active measures to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. These programs directly support USCYBERCOM Integrated Priority List #2 Produce Advanced Cyberspace Infrastructure and #5 Defensive Forces to execute passive and active defense operations at net-speed.

B. Program Change Summary ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**
Previous President's Budget	55.165	36.626	89.183	-	89.183
Current President's Budget	41.441	33.796	62.262	-	62.262
Total Adjustments	-13.724	-2.830	-26.921	-	-26.921
• Congressional General Reductions	-0.035	-			
• Congressional Directed Reductions	-12.000	-2.830			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-1.689	-			
• Adjustments to Budget Years	-	-	-26.921	-	-26.921

Change Summary Explanation

CY5 FY 2020 Base funding in the amount of $20.183 million was aligned to a new program element for Cyber Situational Understanding (SU).
EV5 FY 2019 Base funding in the amount of $2.830 million was decremented from the DCO program, as decided by the Joint APPN Conference due to prior year carryover.
EV5 FY 2020 Base funding in the amount of $26.921 million was reduced due to Army priorities.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 / *CYBER Situational Understanding*

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
CY5: *CYBER Situational Understanding*	-	0.000	0.000	20.183	-	20.183	0.000	0.000	0.000	0.000	0.000	20.183
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Program Element CY5 is a new start beginning in FY20.

A. Mission Description and Budget Item Justification

Cyber SU falls within Line of Effort (LOE) 1 (Unified Network) of the Network Modernization Strategy framework, which incorporates cyber capabilities that support the employment of the network as a weapon system.

CY5 Cyber SU:

Cyber SU supports Cyber Electromagnetic Activity (CEMA) operations by providing visualization of CEMA information to improve planning, coordination, integration and synchronization of cyberspace operations and unified land operations.

Cyber SU provides the Brigade to Corps commanders the visualization of physical (geographically), logical (at a specific network internet protocol), and cyber persona layers (bad actors, from individuals to nation states) of cyberspace based on data/information from multiple sources and sensors to produce a CEMA overlay on the commander's Common Operational Picture (COP) within the Command Post Computing Environment (CPCE). Supporting CEMA, Cyber SU synchronizes and integrates red (enemy), grey (commercial/private sector) and blue (friendly) cyberspace data, and enables collaboration at the tactical edge. Further, in support of the Military Decision Making Process (planning and decision cycles), Cyber SU provides tactical commanders with a thorough understanding of CEMA threats by informing the commander of any cyber related impacts to physical domains, unified land operations, and the overall mission.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Development Engineering ***Description:*** Decomposition of multiple Programs of Record (POR) requirements to initiate development of technical requirement, which will inform government-off-the-shelf (GOTS)/commercial-off-the-shelf (COTS) product evaluation for initial capability procurement and integration. ***FY 2020 Plans:*** FY20 funding will develop the necessary systems engineering/architecture products, middleware and back-end services required to establish an integration environment. In addition, FY20 funds will support software procurement and prototyping of candidate GOTS/COTS products to establish an initial Cyber SU capability to achieve Limited Deployment in FY20.	-	-	15.148

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 / *CYBER Situational Understanding*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Program Executive Office Command, Control and Communications-Tactical will execute these funds. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.			
Title: Systems Test and Evaluation ***Description:*** T&E efforts include the planning and execution of T&E events including Developmental Test, Software Acceptance Testing, Integration Events, Risk Reduction Events, and Initial User Test and Evaluation. ***FY 2020 Plans:*** FY20 funding will provide developmental testing and initial operational test support in preparation for a limited deployment in FY20. Program Executive Office Command, Control and Communications-Tactical will execute these funds. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.	-	-	2.444
Title: Training ***Description:*** The development of training support products will be coordinated with the appropriate US Army Training and Doctrine Command (TRADOC) Capability Managers (TCM), US Army Cyber Command, PORs, and related organizations to develop applicable program of instruction. ***FY 2020 Plans:*** FY20 funding will provide the initial development for training philosophy, methods, and associated products to support a limited deployment in FY20. Program Executive Office Command, Control and Communications-Tactical will execute these funds. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.	-	-	0.118
Title: Systems Engineering/Management ***Description:*** Systems Engineering/Management includes business, technical and logistical staff support and overall management of program execution, major events, reporting, funds execution and contract management.	-	-	2.473

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 **/** *CYBER Situational Understanding*	

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
FY 2020 Plans: FY20 funding will provide funding for program office staff (matrix and contractor) to perform duties necessary to develop, acquire/procure, have a milestone decision review and field Limited Deployment in FY20. Program Executive Office Command, Control and Communications-Tactical will execute these funds. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.			
Accomplishments/Planned Programs Subtotals	-	-	20.183

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

N/A

D. Acquisition Strategy

Cyber SU is an Information Technology (IT) Box program as outlined in the Cyberspace Situational Understanding (Cyber SU) Supporting Army Cyberspace Electromagnetic Activities (CEMA) Information Systems Initial Capability Document (IS-ICD), which was approved 9 March 2018 (Army Requirements Oversight Council [AROC] Memorandum 18-13). TCM Cyber is preparing Core Functionality and Understanding Cyberspace Requirement Definition Package (RDP) in support of Cyber SU. The RDP and subsequent Capability Drops (CDs) are to be approved by the U.S. Army Cyber Center of Excellence in collaboration with U.S. Army Forces Command. Projected RDP approval is 29 January 2019 at the AROC Requirements Board.

Cyber SU will field increasing capability to meet the RDPs and CDs over the program's life cycle. Development of the capability will be depend on several factors, including (but not limited to) availability of commercial and/or government-developed products and how easily the product(s) can be integrated. To that end, the program office intends to evaluate and leverage GOTS/COTS products to the greatest extent and potentially leverage cyber solutions developed by related programs and science and technology efforts (e.g., Defensive Cyberspace Operations (DCO) and Tactical DCO Infrastructure) to satisfy the requirements detailed in the Cyber SU RDPs/CDs. The results of this analysis will inform the final decision on the acquisition strategy, which could include agile developer/operator (DEVOPS) and Section 804. Coordination and integration with complimentary programs and systems-the sources of cyber data feeds-will be an integral part of the program to ensure the data is made available to be consumed by the Cyber SU solution.

Program Executive Office, Command, Control and Communications-Tactical, the Milestone Decision Authority (MDA), approved the Materiel Development Decision on 20 June 2018. The entry point into the acquisition life cycle and projected timeline to a milestone decision will be proposed to the MDA upon receipt and review of the validated RDPs.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 **/** *CYBER Situational Understanding*

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 / *CYBER Situational Understanding*

Management Services ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Systems Engineering/ Management	TBD	TBD : TBD	-	-		-		2.473		-		2.473	0.000	2.473	-
		Subtotal	-	-		-		2.473		-		2.473	0.000	2.473	N/A

Product Development ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Cyber SU Development/ Prototyping	TBD	TBD : TBD	-	-		-		15.148		-		15.148	0.000	15.148	-
		Subtotal	-	-		-		15.148		-		15.148	0.000	15.148	N/A

Support ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Training Development	TBD	TBD : TBD	-	-		-		0.118		-		0.118	0.000	0.118	-
		Subtotal	-	-		-		0.118		-		0.118	0.000	0.118	N/A

Test and Evaluation ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Developmental Test	TBD	TBD : TBD	-	-		-		0.883		-		0.883	0.000	0.883	-
ATEC Support	TBD	US Army Test and Evaluation Command : Aberdeen Proving Ground, MD	-	-		-		0.731		-		0.731	0.000	0.731	-
Accreditation/Certification	TBD	TBD : TBD	-	-		-		0.830		-		0.830	0.000	0.830	-
		Subtotal	-	-		-		2.444		-		2.444	0.000	2.444	N/A

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 **/** *CYBER Situational Understanding*

	Prior Years	FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	-		0.000		20.183		-		20.183	0.000	20.183	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 / *CYBER Situational Understanding*

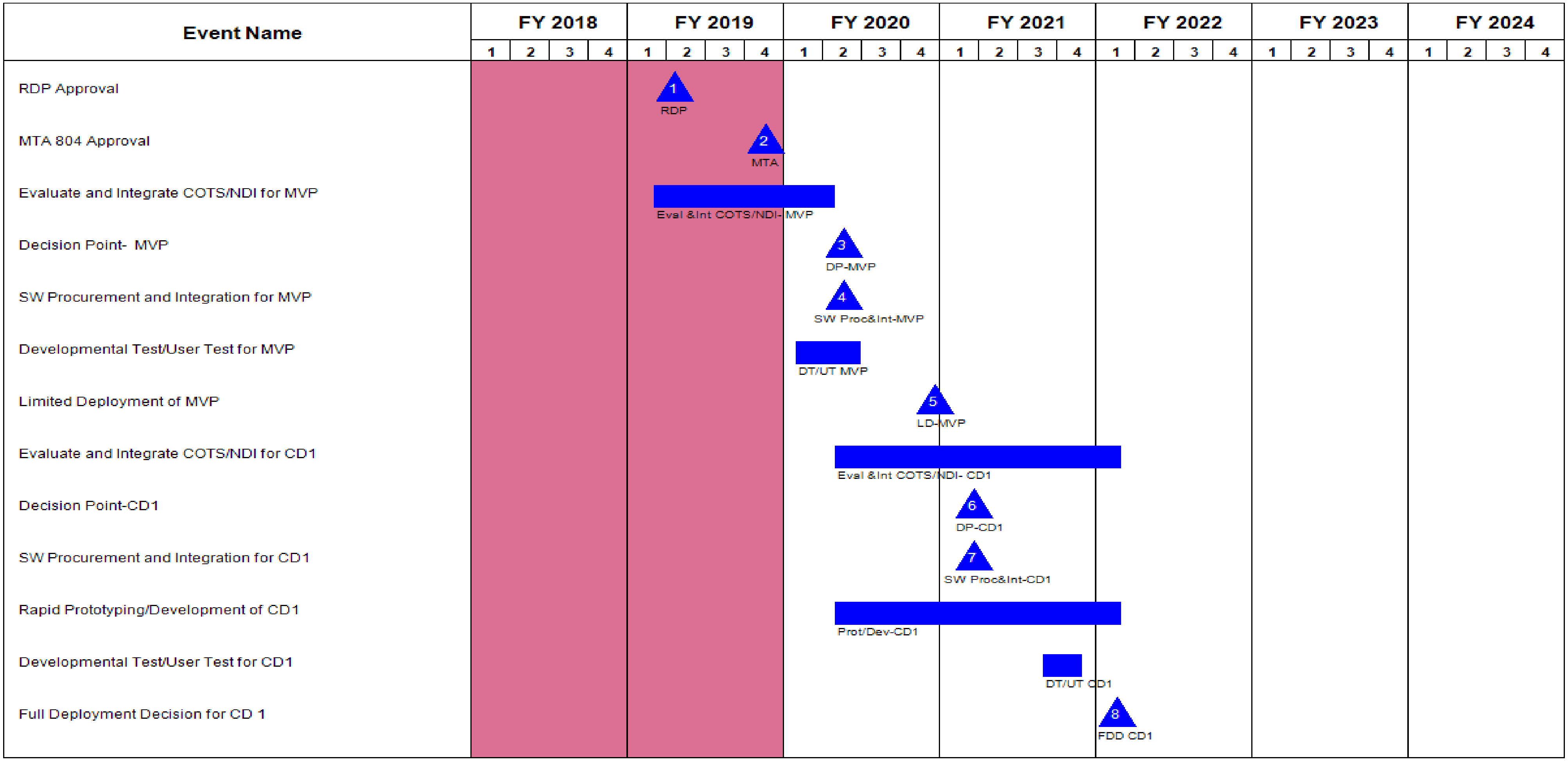

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 / *CYBER Situational Understanding*

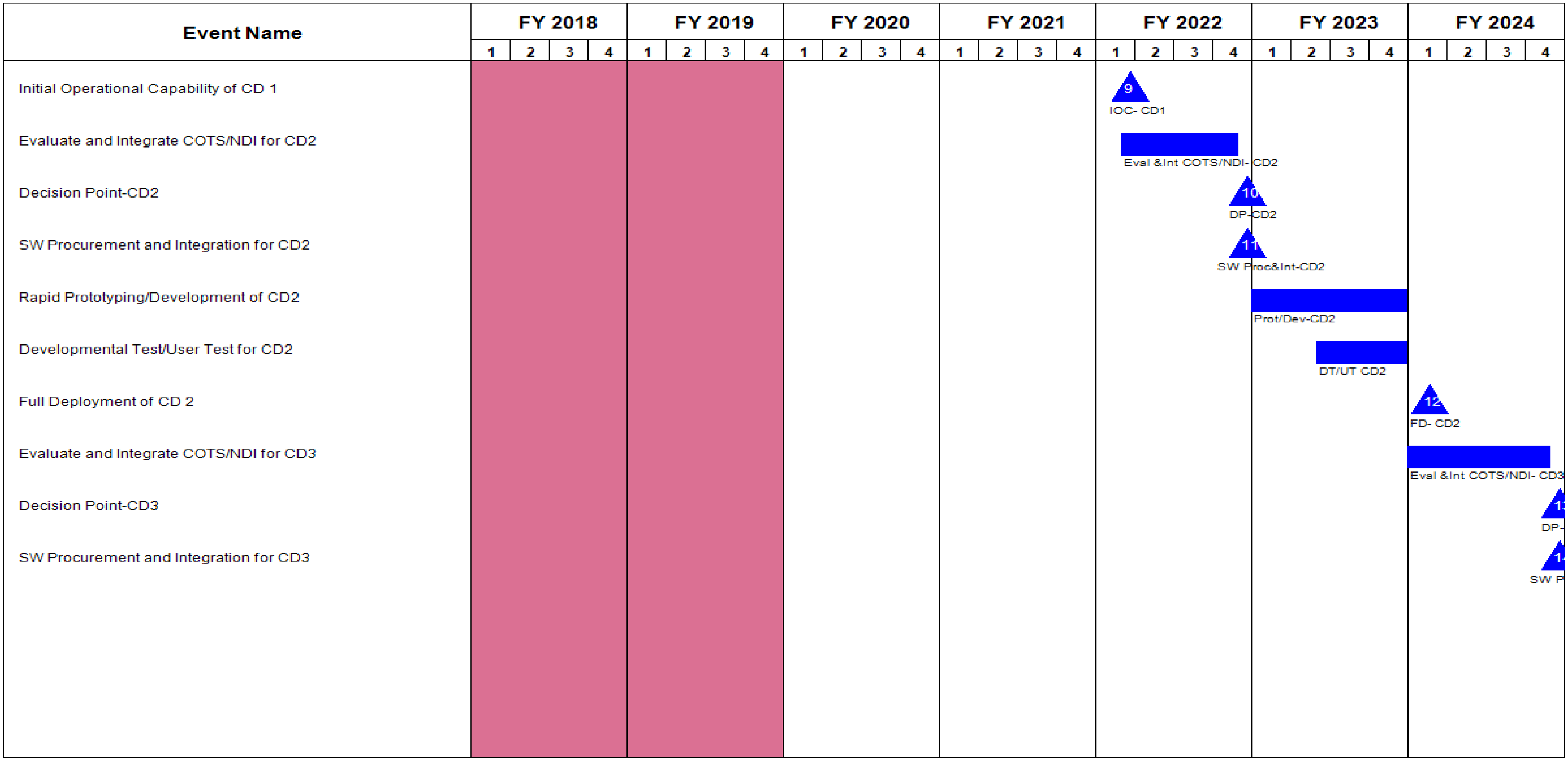

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 **/** *CYBER Situational Understanding*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
RDP Approval	2	2019	2	2019
MTA 804 Approval	4	2019	4	2019
Evaluate and Integrate COTS/NDI for MVP	1	2019	2	2020
Decision Point- MVP	2	2020	2	2020
SW Procurement and Integration for MVP	2	2020	2	2020
Developmental Test/User Test for MVP	1	2020	2	2020
Limited Deployment of MVP	4	2020	4	2020
Evaluate and Integrate COTS/NDI for CD1	2	2020	1	2022
Decision Point-CD1	1	2021	1	2021
SW Procurement and Integration for CD1	1	2021	1	2021
Rapid Prototyping/Development of CD1	2	2020	1	2022
Developmental Test/User Test for CD1	3	2021	4	2021
Full Deployment Decision for CD 1	1	2022	1	2022
Initial Operational Capability of CD 1	1	2022	1	2022
Evaluate and Integrate COTS/NDI for CD2	1	2022	4	2022
Decision Point-CD2	4	2022	4	2022
SW Procurement and Integration for CD2	4	2022	4	2022
Rapid Prototyping/Development of CD2	1	2023	4	2023
Developmental Test/User Test for CD2	2	2023	4	2023
Full Deployment of CD 2	1	2024	1	2024
Evaluate and Integrate COTS/NDI for CD3	1	2024	4	2024
Decision Point-CD3	4	2024	4	2024

Exhibit R-4A, RDT&E Schedule Details: PB 2020 Army	**Date:** March 2019

Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** CY5 **/** *CYBER Situational Understanding*

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
SW Procurement and Integration for CD3	4	2024	4	2024

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 / *Defensive CYBER Operations*

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
EV5: *Defensive CYBER Operations*	-	41.441	33.796	42.079	-	42.079	29.738	92.873	94.974	90.000	0.000	424.901
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Defensive Cyber Operations - Tactical DCO Infrastructure (TDI)- (PEO C3T)
Defensive Cyber Operations - Cyberspace Analytics - (PEO EIS)
Defensive Cyber Operations - Mission Planning - (PEO EIS)
Defensive Cyber Operations - Tools Suite - (PEO EIS)
Defensive Cyber Operations - Garrison DCO Platform - (PEO EIS)
Defensive Cyber Operations - Deployable DCO System - (PEO EIS)
Defensive Cyber Operations - User Activity Monitoring - (PEO EIS)
Defensive Cyber Operations - Forensics and Malware - (PEO EIS)
Defensive Cyber Operations - Advanced Sensors - (PEO EIS)
Defensive Cyber Operations - Threat Emulation - (PEO EIS)
Defensive Cyber Operations - Counter Infiltration - (PEO EIS)
Defensive Cyber Operations - Forge - (PEO EIS)
Defensive Cyber Operations - Rapid Cyber Prototyping - (ARCYBER)

A. Mission Description and Budget Item Justification

Defensive Cyber Operations (DCO) falls within Line of Effort (LOE) 1 of the Network Modernization Strategy framework, which incorporates cyber capabilities that support the employment of the network as a weapon system.

FY 2020 RDTE DCO efforts consists of the following critical capabilities:

-Tactical DCO Infrastructure (TDI): System (automated on boot infrastructure to deploy DCO Tools on the Tactical Server Infrastructure (TSI)) which resides within the Command Post, at Brigade through Corps, for both organic Cyber Network Defenders as well as remote access by CPT to support defense of the tactical network (PEO C3T)
-Cyberspace Analytics (CA): Identification of threat trends, behavior patterns, and Techniques Tactics and Procedures (TTPs) relative to associated portions of the information environment. The cyberspace analytics capability offers an integrated platform that can be leveraged across all security enclaves (NIPRNET, SIPRNET, and JWICS) to enhance both DCO and Department of Defense Information Network (DODIN) operations (PEO EIS)
-Mission Planning (MP): An application-based, scalable warfighting capability for Army DCO mission command and planning at the global, regional, and local levels. DCO MP enables integration, coordination, and synchronization of supported and supporting cyberspace defenders (PEO EIS)

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

-Tools Suite: Flexible and dynamic suite of warfighting capabilities that enable Cyber Mission Forces and other cyberspace defenders to perform functional categories consisting of site survey; risk assessment; observation; intel support; counter-mobility; developer/operator (DEVOPS), event correlation, and command and control (PEO EIS)
-Garrison DCO Platform (GDP): Prepositioned, dedicated compute and storage resources residing at high/extremely high risk installations. Provides cyberspace defenders a remote maneuver capability in order to augment and/or support cyberspace defenders existing at designated bases, posts, camps, or stations by preserving an organization's ability to utilize mission critical data, networks, net-centric capabilities, and other designated systems (PEO EIS)
-Deployable DCO System (DDS): A deployable kit, with dedicated compute and storage for austere environments that do not have prepositioned infrastructure or locations for which prepositioned DCO resources do not provide adequate capacity. The DDS allows global cyberspace defenders (e.g. CPTs) the ability to jump into a network, physically, onsite and gain a position of advantage to augmenting organic local and/or regional cyberspace defenders (PEO EIS)
-User Activity Monitoring (UAM): The primary capability within the Army's overall insider threat detection (InT) program. UAM is a software-based, scalable solution that proactively identifies and mitigates internal risks associated with the theft and misuse of critical, mission essential data. UAM utilizes full-spectrum solutions to assess, deter, deny, defend, defeat, and evolve against the insider threat hub (PEO EIS)
-Forensics and Malware Analysis (F&MA): Warfighting capability adheres to the global standard in digital investigation technology for global or regional cyberspace defenders who need to conduct efficient, forensically-sound, data collection and examination either remotely or locally using a repeatable and defensible process. Forensics gives cyberspace defenders the ability to triage by quickly viewing and searching potential evidence in order to determine whether further examination is warranted (PEO EIS)
-Advanced Sensors: Real-time discovery of specific advanced or sophisticated cyber threats and vulnerabilities on a critical system or segment of the network. Advanced sensors provides an automated monitoring and incident handling capability lower in the network architecture (access layer) to conduct over-watch for high-risk units or systems that normally operate out of view ("last mile") from traditional security or DCO measures (PEO EIS)
-Threat Emulation: Software and hardware based suite of tools used by a Cyber OPFOR to gain access to evaluated networks and systems using multi-vectors of unknown ("blackbox"), partially known ("graybox"), or known ("whitebox") access methods. Enables the implementation of real world threat tactics, techniques, and procedures against risk areas in order to reveal extremely high-risk security exposures and demonstrate the operational impact of a potential attack (PEO EIS)
-Counter Infiltration: Software/hardware array of components that retrogrades mission critical assets from virtual areas under a cyber threat actor's control using stealth, deception, surprise, or clandestine movements. The capability allows commanders and leaders to trade space for time by slowing down the advanced persistent threat's without becoming decisively engaged (PEO EIS)
-Forge: Provides integration and assessment capabilities during the development and integration phases of operations. DCO program will leverage non-FAR based Other Transaction Authorities (OTA) to solicit prototype/new technologies for consideration of procurement decisions.
-Rapid Cyber Prototyping: Rapidly develops cyber capabilities identified by the Cyber Mission Forces (CMF) in order to counter advanced, persistent, and sophisticated cyber threats (ARCYBER)

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Title: Defensive Cyber Operations (DCO) - Tactical DCO Infrastructure (TDI) - (PEO C3T) ***Description:*** TDI is a system (automated on boot infrastructure to deploy DCO Tools on the Tactical Server Infrastructure (TSI)) which resides within the Command Post, at Brigade through Corps, for both organic Cyber Network Defenders as well as remote access by CPT to support defense of the tactical network. (PEO C3T)	9.527	6.343	3.282

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
FY 2019 Plans: The FY19 funding will support completion of development engineering, integration and testing of the Minimum Viable Product (MVP) capability release of TDI. ***FY 2020 Plans:*** FY20 funding will support the development engineering, integration and testing of Capability Drop 1 (CD1). CD1 will upgrade the DCO tools integrated on the TSI, expand the sensor architecture to more command post applications, thus increasing the tactical commander?s defensive cyber posture. This effort?s funding will be executed by Program Executive Office for Command, Control and Communications-Tactical. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 increase due to continuous need of integrating new DCO tools within the TSI and expanding the Cyber sensor architecture to more command post applications.			
Title: Defensive Cyber Operations (DCO) - Cyberspace Analytics - (PEO EIS) ***Description:*** The cyberspace analytics capability offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate reconnaissance activities meant to discover the presence of advanced or sophisticated cyberspace threats and vulnerabilities. The cyberspace analytics capability offers an integrated platform that can be leveraged across all security enclaves (NIPRNET, SIPRNET, and JWICS) in order to ingest, process, store, share, and visualize multiple petabyte, distributed data sets. ***FY 2019 Plans:*** FY19 focuses on creating a distributed analytic environment. This environment will allow for query of data that is resident at the Tactical, Deployable, or Garrison locations. Additionally FY19 will see the development of a lightweight analytic engine that can be placed on Tactical, Deployable, or Garrison systems to allow local operators immediate access to emerging threat data and forward sensor data. Additional analytics that will be developed include: Data Discovery, Data Discovery Model, Distributed Query, Whitelist/Blacklist, Single Sign-On Analytic, Greyspace Analysis Analytic, Data Correlation Analytic and Reduced Alert Overhead Analytic. ***FY 2020 Plans:*** Continue improvements to the cyberspace analytic/big data platform solution by adding additional data parsers that support behavioral, prescriptive, and predictive analytics. Improvements will also include provisioning of graphical techniques to see patterns in data that might not otherwise be obvious. The Army will additionally increase the use of embedded capabilities consisting of tools that are integrated with other applications, operating as a component of the application rather than a separate platform. Critical to success is the maturation of DEVOPS and DEVOPS tools to support rapid cyberspace analytical development.	23.234	9.129	10.400

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Moreover, the Army will continue to ensure the confidentiality and integrity of data residing on the platform by improving or adding identify and access management, as well as cross domain data transfer solutions. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Increase due to continuous improvements to the cyberspace analytic/big data platform solution by adding additional data parsers that support behavioral, prescriptive, and predictive analytics.			
Title: Defensive Cyber Operations (DCO) - Mission Planning - (PEO EIS) ***Description:*** DCO Mission Planning (DCOMP) integrates network security requirements, intelligence, and vulnerability analyses, with a commander?s operation order (e.g. mission statement, commander?s intent, planning guidance, initial commander critical information requirements/essential elements of friendly information, and assumptions), and other military decision-making process outputs, and actions to identify key terrain in cyberspace and mission critical assets; determine probable attack vectors; and produce a set of relevant internal defense measures, triggers, and decision points. The result is the automated production of the appropriate operations order (OPORD) appendix, which is then war-gamed in a simulation engine for evaluation and improvement. DCOMP utilizes the final OPORD to rapidly provision necessary platforms so cyberspace defenders can execute mission in near real-time. ***FY 2019 Plans:*** FY19 integrates the cyber analytics capability through an interface into the mission planning solutions as well as integration of Cyber Protection Team Tool suites to allow for seamless transitions from one tool to another during a mission. Additional functionality such as a team communicator, allowing teams to collaborate and share site picture, as well as automated planner capabilities that ingest operations order data, deconstruct and recommend applications for the mission will be added. ***FY 2020 Plans:*** Continued improvements to DCOMP will include the ability to map a network with a commander's military or business operation in order to automate the identification of mission relevant terrain in cyberspace. This will support the insertion of a battle tracking capability that monitors mission execution and provides a status on mission performance and effectiveness. Additionally, the Army will seek to integrate a cross domain solution and develop a wargaming module (to include Persistent Cyber Training Range integration). Finally, development efforts will focus on the creation of a controller module that can take the output of the military decision making process and automatically array corresponding infrastructure, platforms, and tools against the mission in a way that readies the capabilities before the virtual or on-site arrival of cyberspace defenders. The Army will ensure the capability maintains access to applicable cyber symbology and geospatial information Infrastructure Controller. ***FY 2019 to FY 2020 Increase/Decrease Statement:***	6.613	10.322	9.100

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Provides limited continuous improvements to DCOMP including the ability to map a network with a commander's military or business operation in order to automate the identification of mission relevant terrain in cyberspace.			
Title: Defensive Cyber Operations (DCO) - Tools Suite - (PEO EIS) ***Description:*** The Army employs its tools within a prepositioned or deployable environment and organizes them by function. DCO tools are functionality aligned to identified performance characteristics. Functional categories consist of site survey; risk assessment; observation; intel support; counter-mobility; DEVOPS, event correlation, and command and control. Tools are encapsulated into purpose-built platforms: Publicly available security distributions (managed by open source teams outside of the Army?s direct control), virtual machines (VM) containing licensed tools (containerized with an operating system (OS) and vendor-licensed software installed), and Orchestrated VMs (VMs exist with just enough OS to be able to receive instructions from a host cloud computing OS). Facilitates evaluations and assessments in a closed, controlled repeatable environment on virtualized infrastructure of common services, toolsets, and/or platforms for simplifying and standardizing designs and processes, as well as codifying functions and services into an ontology. ***FY 2019 Plans:*** Support the Cyber Protection Teams (CPTs) to do real time writing, modification, and customization of software code and algorithms for analytics in response to mission changes; resourcing includes software for testing of newly written code, access to contracted industry experts and research facility support for creation of tools in response to emerging threats ***FY 2020 Plans:*** Operational development environment that provides Soldiers access to Open Source software code as well as hardware in a toolbox configuration allowing them to build the DCO capabilities in response to real-time threats. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** No significant changes.	0.689	1.548	1.600
Title: Defensive Cyber Operations (DCO) - Garrison DCO Platform - (PEO EIS) ***Description:*** The Garrison DCO Platform consists of pre-positioned dedicated compute and storage resources residing at high risk locations. This infrastructure serves as a remote capability for cyberspace defenders. Remote management software is utilized to provide cross-domain access to all defensive cyber platforms, serving as the maneuver capability for defenders. ***FY 2019 Plans:*** The enhancement of remote management capability to include passive network mapping, remote management of advanced sensors, and interface with Reserve and National Guard capabilities. ***FY 2020 Plans:***	0.689	0.288	0.950

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Continue to improve the ability to tap, filter, process and manipulate traffic all in a cloud environment. Continue to evaluate less expensive options for packet processing, deep packet inspection, and load balancing. Prototyping ?extreme architectures? that string together multiple microprocessors and establish software-based architectures to harness the processing power inherent to the instantiation of numerous platforms. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY19 funding support the enhancement of remote management capability to include passive network mapping, remote management of advanced sensors, and interface with Reserve and National Guard capabilities. FY20 will be for new emerging prototyping technology only.			
Title: Defensive Cyber Operations (DCO) - Deployable DCO System - (PEO EIS) ***Description:*** A deployable (fly away) kit, with dedicated compute and storage for austere environments that do have prepositioned infrastructure or locations for which prepositioned DCO resources do not provide adequate capacity. The DDS allows global cyberspace defenders (e.g. CPTs) the ability to jump into a network, physically, onsite and gain a position of advantage to augmenting organic local and/or regional cyberspace defenders. ***FY 2019 Plans:*** Provide engineering, prototyping, and test and evaluation support for Deployable DCO System. ***FY 2020 Plans:*** Improve on data ingest speeds, data staging options, and develop capabilities for remote operations (to include executive communications for Army National Guard and Reserved). Continue to improve the ability to tap, filter, process, and manipulate traffic all in a cloud environment. Continue to evaluate less expensive options for packet processing, deep packet inspection, and load balancing. Prototype smaller kits for initial and sustained configurations and determine viability of lite-kit for quick reaction, very short mission durations. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** AROC approved on 16 Jan 18. FY20 procures engineering, prototyping, and test and evaluation support for DDS.	0.689	0.288	0.950
Title: Defensive Cyber Operations (DCO) - User Activity Monitoring - (PEO EIS) ***Description:*** The primary capability within the Army's overall insider threat detection (InT) program. UAM is a software-based, scalable solution that proactively identifies and mitigates internal risks associated with the theft and misuse of critical, mission essential data. UAM utilizes full-spectrum solutions to assess, deter, deny, defend, defeat, and evolve against the insider threat hub. ***FY 2019 Plans:***	-	0.297	2.764

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Provides data audit and trigger capabilities for all users on both the SIPRNET, JWICS, and special access program environments, as well as privilege users on the NIPRNET. Integrates behavioral analysis and associated data sources with the UAM capability. ***FY 2020 Plans:*** Implementation of UAM for all Soldiers, civilian, and contractors with access to Joint Worldwide Intelligence Communication System (JWICS) and SIPRNet. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Implementation of UAM for all Soldiers, civilian, and contractors with access to Joint Worldwide Intelligence Communication System (JWICS) and SIPRNet.			
Title: Defensive Cyber Operations (DCO) - Forensics and Malware Analysis - (PEO EIS) ***Description:*** Warfighting capability adheres to the global standard in digital investigation technology for global or regional cyberspace defenders who need to conduct efficient, forensically-sound, data collection and examination either remotely or locally using a repeatable and defensible process. Forensics gives cyberspace defenders the ability to triage by quickly viewing and searching potential evidence in order to determine whether further examination is warranted ***FY 2019 Plans:*** Development efforts will provide initial capabilities under a program to the ARCYBER Forensics and Malware Cell, the Army's five (5) Regional Cyber Centers, the Cyber Protection Brigade Advanced Threat Analysis and Mitigation Cell, and potentially Army National Guard and Army Reserve units. Initial capabilities delivered will be those that enable live-box forensics either remotely or locally. Additionally, the solution will provide analysts a semi-automated capability to analyze file systems, timelines, network traffic, web histories, recycle bins, memory, disks, logs, registries, and other artifacts. The solution will additionally consist of a software-based application to analyze malicious code in a sandbox-like, virtual environment in order to conduct real-time, automated and dynamic malware decomposition and behavior analysis. ***FY 2020 Plans:*** Provides cyberspace defenders ability to rapidly triage an incident, assists with determining subsequent actions required to collect, process, search and analyze evidence from multiple media/devices. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 provides key enhancements which include improved reporting, integration with existing cybersecurity solutions, increased OS and file system support, a more intuitive user interface, and advanced case management.	-	0.288	0.530
Title: Defensive Cyber Operations (DCO) - Advanced Sensors - (PEO EIS) ***Description:*** Real-time discovery of specific advanced or sophisticated cyber threats and vulnerabilities on a critical system or segment of the network. Advanced sensors provides an automated monitoring and incident handling capability lower in the	-	-	3.250

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
network architecture (access layer) to conduct over-watch for high-risk units or systems that normally operate out of view ("last mile") from traditional security or DCO measures. ***FY 2020 Plans:*** Develop initial capability that is a simple, very small, low-cost solution employed along likely avenues of approach (physical and logical). The initial capability will provide an automated surveillance and counter-mobility solution lower in the network architecture (access layer) to conduct over-watch for high-risk units or systems that normally operate out of view (?last mile?) from traditional, routine security or DCO measures. The primary measure of effectiveness for an advanced cyber sensor is real-time discovery of specific advanced or sophisticated cyber threats and vulnerabilities on a critical system or segment of the network. When a TTP is detected, advanced sensors can execute a myriad of tailored response actions (block, neutralize, deceive, redirect, etc.) on the associated payload. The result is an increased ability to interrupt the adversary at the beginning of the cyber kill chain by employing counter-measures during the reconnaissance and weaponization phases; and neutralizing and/or deceiving the adversary during the delivery, exploitation, and installation phases. To enable this approach, advanced cyber sensors incorporate indications and warnings (I&W) algorithmically to provide identification and reporting of time-sensitive information on developments that could involve a threat to the network. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.			
Title: Defensive Cyber Operations (DCO) - Threat Emulation - (PEO EIS) ***Description:*** Software and hardware based suite of tools used by a Cyber Opposing Forces to gain access to evaluated networks and systems using multi-vectors of unknown ("blackbox"), partially known ("graybox"), or known ("whitebox") access methods. Enables the implementation of real world threat tactics, techniques, and procedures against risk areas in order to reveal extremely high-risk security exposures and demonstrate the operational impact of a potential attack. ***FY 2020 Plans:*** Develop initial capability for designated cyberspace defenders to conduct threat emulation activities IAW applicable concepts of operations and regulations. Initial capabilities will consists of a solution used to gain access to evaluated networks and systems through multi-vectors of unknown, partially known, or known exploits. Threat Emulation will enable the implementation of real world threat tactics, techniques, and procedures against risk areas in order to reveal critical security exposures. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.	-	-	3.403
Title: Defensive Cyber Operations (DCO) - Counter Infiltration - (PEO EIS)	-	-	2.850

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Description: Software/hardware array of components that retrogrades mission critical assets from virtual areas under a cyber threat actor's control using stealth, deception, surprise, or clandestine movements. The capability allows commanders and leaders to trade space for time by slowing down the advanced persistent threat's without becoming decisively engaged. ***FY 2020 Plans:*** Develop initial capability consisting of an array of components that retrograde mission critical assets from virtual areas under a cyberspace threat actor?s control using stealth, deception, surprise, or clandestine movements. The capability will change the identity of assets between relatively small time periods based on mathematical algorithms. Mission critical assets within the same virtual area of operations will share certain, common information, which results in an asset not only knowing it's next identity and location, but it is additionally aware of the next identity and location of all other mission critical systems. As time progresses, systems within the same Area of Operations retrograde in unison. Characteristics of a system that can change consist of Internet Protocol address, media access control address, ports, protocol, services, computer name, etc. The capability will allow commanders and leaders to trade space for time by slowing down the advanced persistent threat?s without becoming decisively engaged. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.			
Title: Defensive Cyber Operations (DCO) - Forge (Integration) - (PEO EIS)	-	5.293	2.000
Description: The Forge is a physical location that provides integration and assessment capabilities during the development and integration phases of operations. Full Operational Capability (FOC) by FY20. ***FY 2019 Plans:*** At the Forge, the DCO program will leverage non-FAR based Other Transaction Authorities (OTA) to solicit prototype/new technologies for consideration of procurement decisions. OTAs will provide access to industry (large, small, and by definition non-traditional defense contractors), academia, as well as Government laboraties. The Forge is also the primary location for the administration of a rapid prototyping process referred to as the Cyberspace Real-Time Acquisition Prototype Innovation Development (C-RAPID). ***FY 2020 Plans:*** Continues to provide DCO Suite of Complimentary Systems (DSCS) integration and testing at the Forge. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** The Forge will be at FOC in FY20. FY20 decrease due to funding reprioritization.			
Title: Defensive Cyber Operations (DCO) - Rapid Cyber Prototyping - (ARCYBER)	-	-	1.000

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Description: Rapidly develops cyber capabilities that cannot be acquired through traditional acquisition process in order to counter advanced, persistent, and sophisticated cyber threats. ***FY 2020 Plans:*** Supports rapid prototyping, developmental assessment and operational fielding of capabilities and responses to Cyber Mission Forces Cyber Needs Form. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** New start in FY20.			
Accomplishments/Planned Programs Subtotals	41.441	33.796	42.079

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• B63103: *DEFENSIVE CYBER TOOLS*	53.436	51.343	61.962	-	61.962	69.655	95.504	104.568	114.000	Continuing	Continuing
• N/A: *OMA Defensive Cyber Operations (MDEP MU2Z SAG 432612)*	0.640	3.000	5.000	-	5.000	5.000	5.000	-	-	Continuing	Continuing

Remarks

OPA PE B63103 for DCO procurement, fielding and training.
OMA SAG 432612 for DCO License Renewals and non-traditional sustainment.
OMA SAG 435106 for Civilian Pay was established by the Department starting in FY19 due to Reimbursable to Direct conversion for DCO.

D. Acquisition Strategy

The Defensive Cyber Operations (DCO) will support multiple programs. The Army conducted Materiel Development Decisions (MDD) in FY18 based upon the DCO Information System Initial Capabilities Document (IS ICD). DCO will develop and integrate the DCO Suite of Complimentary Systems (DSCS) using an incremental evolutionary acquisition approach that employs iterative development and acquisition reform principals, complying with the 1996 Clinger-Cohen Act. The approach leverages prototyping using the Operational Needs Statement (ONS) high-level objectives as a bridging strategy to establish the acquisition programs. The DSCS was initiated via four (4) ONSs, which have transitioned into Program of Records (PORs).

System designs focus on open architecture and open source capabilities. Department will utilize Evolutionary Acquisition (Delivery, Assess, Deploy, Learn and Iterate). Implementation of a modular design to maximize innovation through continuous releases. Modules will be refined by industry as a component through adoption of

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

prototypes. Each program will have a prime integrator (single contractor) that integrates the new modules. The Government will assess and create prototypes employing a combination of Government entities and commercial vendors via Other Transaction Authority contract vehicle.

The Tactical DCO Infrastructure (TDI) program's MDD was conducted in 2QFY18. Based on the validated DCO IS ICD and the TDI Requirements Definition Package (RDP), the Milestone Decision Authority (MDA) signed the Acquisition Decision Memorandum (ADM) delegating TDI as an ACAT III program. TDI will leverage the Simplified Acquisition Plan (SAMP) approach and will use acquisition tailoring in preparing for MSB, scheduled for 3QFY19. To support the Department's evolutionary acquisition approach, the TDI program office will develop the software infrastructure and deployment scripts that provide a technological solution that is converged with the Tactical Server Infrastructure in a series of incremental builds to deliver capabilities that align with DCO priorities. Execution of the TDI program will be a combination of government entities and commercial vendors.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

Management Services ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Defensive Cyber Operations - Tactical DCO Infrastructure (TDI) (PEO C3T)	C/CPFF	PEO C3T : Aberdeen Proving Ground (APG), MD	4.188	3.509		2.282		1.180		-		1.180	Continuing	Continuing	Continuing
Defensive Cyber Operations (DCO) - Cyberspace Analytics (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	0.228	0.324		0.299		0.700		-		0.700	Continuing	Continuing	Continuing
Defensive Cyber Operations - Tools Suite (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	-	0.189		0.288		0.100		-		0.100	Continuing	Continuing	Continuing
Defensive Cyber Operatons - Garrison DCO Platform (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	0.724	0.189		0.288		0.100		-		0.100	Continuing	Continuing	Continuing
Defensive Cyber Operatios - Mission Planning (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	0.219	0.323		0.298		0.200		-		0.200	Continuing	Continuing	Continuing
Defensive Cyber Operations - Deployable DCO System (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	-	0.189		0.288		0.100		-		0.100	Continuing	Continuing	Continuing
Defensive Cyber Operations - Forensics and Malware (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	-	-		0.288		-		-		-	0.000	0.288	-
Defensive Cyber Operations - User Activity Monitoring (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	-	-		0.297		-		-		-	0.000	0.297	-
Defensive Cyber Operations - Forge (PEO EIS)	C/FFP	PEO EIS : Ft Belvoir, VA	-	-		5.293		2.000		-		2.000	0.000	7.293	-
		Subtotal	5.359	4.723		9.621		4.380		-		4.380	Continuing	Continuing	N/A

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

Product Development ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Defensive Cyber Operations - Tactical DCO Infrastructure (TDI) (PEO C3T)	C/CPFF	SEC and I2WD : Aberdeen Proving Ground (APG), MD	1.631	5.190		3.453		1.787		-		1.787	Continuing	Continuing	Continuing
Defensive Cyber Operations - Cyberspace Analytics (PEO EIS)	C/FFP	ACC-RI : IL	3.700	17.987	Jan 2018	8.830	Dec 2018	8.500		-		8.500	Continuing	Continuing	Continuing
Defensive Cyber Operations - Tools Suite (PEO EIS)	C/TBD	ACC-Rock Island (ACC-RI) : IL	-	-		1.260		1.300		-		1.300	Continuing	Continuing	Continuing
Defensive Cyber Operations - Garrison DCO Platform (PEO EIS)	C/FFP	ACC-RI : IL	2.060	-		-		0.700		-		0.700	Continuing	Continuing	Continuing
Defensive Cyber Operations - Garrison DCO Platforms (PEO EIS)	C/Various	ACC-PI : NJ	9.690	-		-		-		-		-	Continuing	Continuing	Continuing
Defensive Cyber Operations - Deployable DCO System (PEO EIS)	C/Various	ACC-RI : IL	-	-		-		0.700		-		0.700	Continuing	Continuing	Continuing
Defensive Cyber Operations - Mission Planning (PEO EIS)	C/CPFF	ACC-RI : IL	-	-		10.024	Nov 2018	8.900		-		8.900	Continuing	Continuing	Continuing
Defensive Cyber Operations - User Activity Monitoring (PEO EIS)	C/T&M	ACC-RI : IL	-	-		-		2.764		-		2.764	Continuing	Continuing	Continuing
Defensive Cyber Operations - Forensics and Malware (PEO EIS)	C/TBD	ACC-RI : IL	-	-		-		0.530		-		0.530	Continuing	Continuing	Continuing
Defensive Cyber Operations - Advanced Sensors (PEO EIS)	C/TBD	ACC-RI : IL	-	-		-		3.250		-		3.250	Continuing	Continuing	Continuing
Defensive Cyber Operations - Threat Emulation (PEO EIS)	C/TBD	ACC-RI : IL	-	-		-		3.403		-		3.403	Continuing	Continuing	Continuing

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

Product Development ($ in Millions)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Defensive Cyber Operations - Counter Infiltration (PEO EIS)	C/TBD	ACC-RI : IL	-	-		-		2.850		-		2.850	Continuing	Continuing	Continuing
Defensive Cyber Operations - Rapid Cyber Prototyping (ARCYBER)	C/TBD	ACC-RI : IL	-	-		-		1.000		-		1.000	0.000	1.000	-
Defensive Cyber Operations - Mission Planning (PEO EIS)	MIPR	USAF, AFMC AIR FORCE RESEARCH LAB : NY	10.095	4.425	Apr 2018	-		-		-		-	0.000	14.520	-
Subtotal			27.176	27.602		23.567		35.684		-		35.684	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Defensive Cyber Operations - Tactical DCO Infrastructure (TDI) (PEO C3T)	C/TBD	Aberdeen Proving Ground : MD	-	0.828		0.608		0.315		-		0.315	Continuing	Continuing	Continuing
Defensive Cyber Operations - Cyberspace Analytics (PEO EIS)	MIPR	ATEC : MD	-	4.923		-		1.200		-		1.200	0.000	6.123	-
Defensive Cyber Operations - Tools Suite (PEO EIS)	MIPR	ATEC : MD	-	0.500		-		0.200		-		0.200	0.000	0.700	-
Defensive Cyber Operations - Garrison DCO Platform (PEO EIS)	MIPR	ATEC : MD	-	0.500		-		0.150		-		0.150	0.000	0.650	-
Defensive Cyber Operations - Deployable DCO System (PEO EIS)	MIPR	ATEC : MD	-	0.500		-		0.150		-		0.150	0.000	0.650	-

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

Test and Evaluation ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Defensive Cyber Operations - Mission Planning (PEO EIS)	MIPR	ATEC : MD	-	1.865		-		-		-		-	0.000	1.865	-
		Subtotal	-	9.116		0.608		2.015		-		2.015	Continuing	Continuing	N/A

	Prior Years	**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	32.535	41.441		33.796		42.079		-		42.079	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 / *Defensive CYBER Operations*

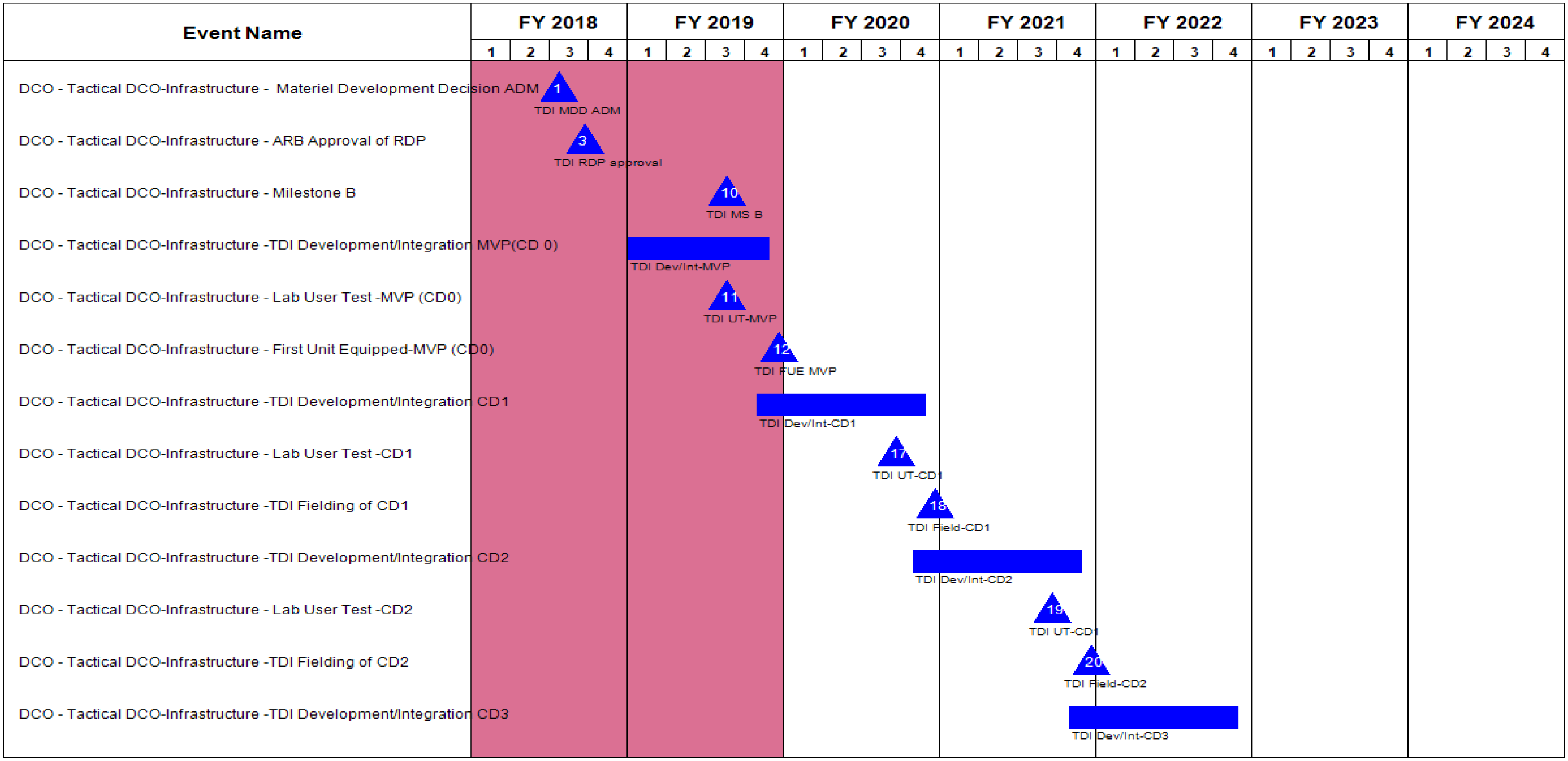

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A / *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 / *Defensive CYBER Operations*

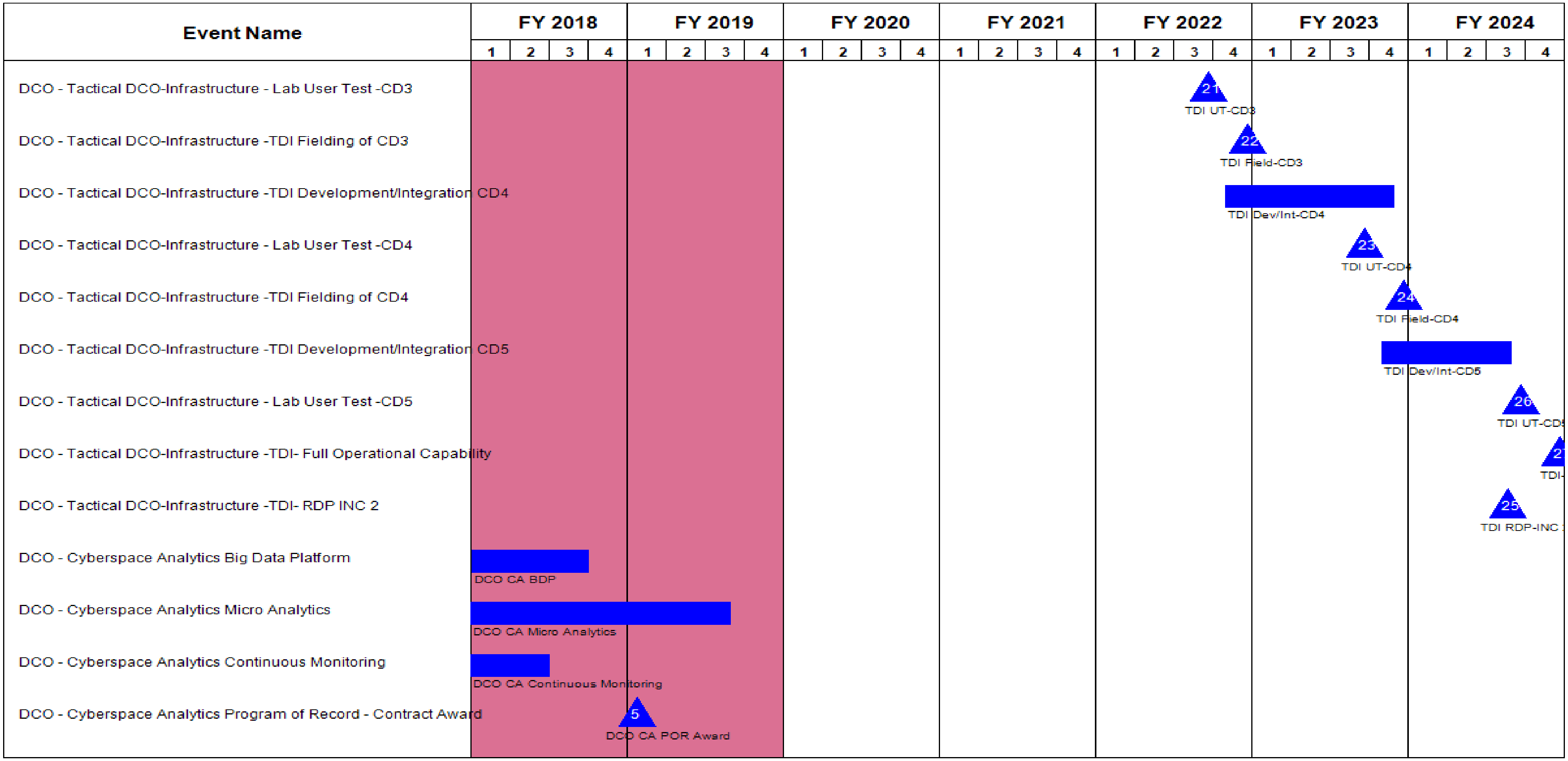

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 5	**R-1 Program Element (Number/Name)** PE 0605041A */ Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 */ Defensive CYBER Operations*

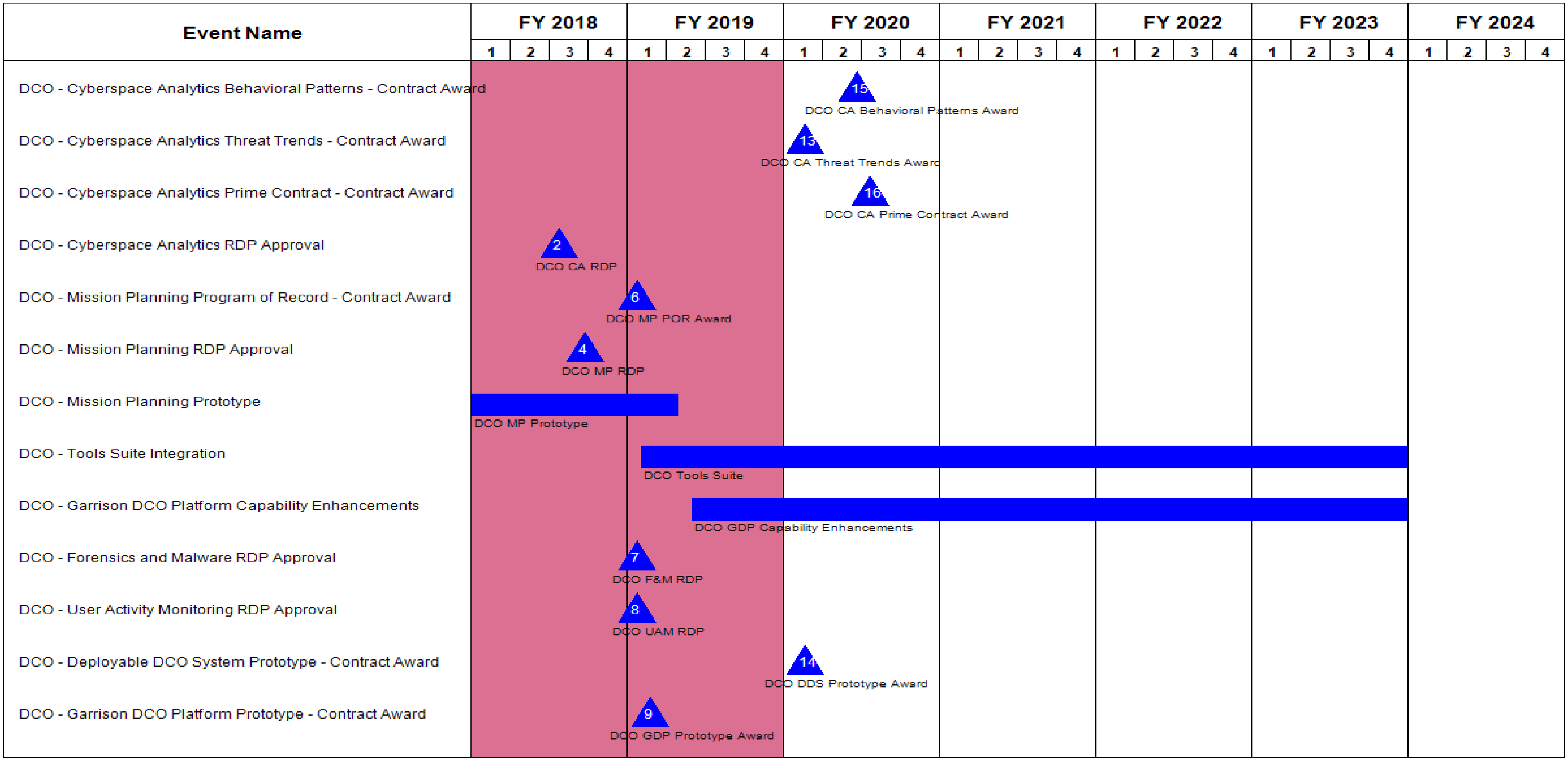

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

Schedule Details

	Start		**End**	
Events	**Quarter**	**Year**	**Quarter**	**Year**
DCO - Tactical DCO-Infrastructure - Materiel Development Decision ADM	3	2018	3	2018
DCO - Tactical DCO-Infrastructure - ARB Approval of RDP	3	2018	3	2018
DCO - Tactical DCO-Infrastructure - Milestone B	3	2019	3	2019
DCO - Tactical DCO-Infrastructure -TDI Development/Integration MVP(CD 0)	1	2019	4	2019
DCO - Tactical DCO-Infrastructure - Lab User Test -MVP (CD0)	3	2019	3	2019
DCO - Tactical DCO-Infrastructure - First Unit Equipped-MVP (CD0)	4	2019	4	2019
DCO - Tactical DCO-Infrastructure -TDI Development/Integration CD1	4	2019	4	2020
DCO - Tactical DCO-Infrastructure - Lab User Test -CD1	3	2020	3	2020
DCO - Tactical DCO-Infrastructure -TDI Fielding of CD1	4	2020	4	2020
DCO - Tactical DCO-Infrastructure -TDI Development/Integration CD2	4	2020	4	2021
DCO - Tactical DCO-Infrastructure - Lab User Test -CD2	3	2021	3	2021
DCO - Tactical DCO-Infrastructure -TDI Fielding of CD2	4	2021	4	2021
DCO - Tactical DCO-Infrastructure -TDI Development/Integration CD3	4	2021	4	2022
DCO - Tactical DCO-Infrastructure - Lab User Test -CD3	3	2022	3	2022
DCO - Tactical DCO-Infrastructure -TDI Fielding of CD3	4	2022	4	2022
DCO - Tactical DCO-Infrastructure -TDI Development/Integration CD4	4	2022	4	2023
DCO - Tactical DCO-Infrastructure - Lab User Test -CD4	3	2023	3	2023
DCO - Tactical DCO-Infrastructure -TDI Fielding of CD4	4	2023	4	2023
DCO - Tactical DCO-Infrastructure -TDI Development/Integration CD5	4	2023	3	2024
DCO - Tactical DCO-Infrastructure - Lab User Test -CD5	3	2024	3	2024
DCO - Tactical DCO-Infrastructure -TDI- Full Operational Capability	4	2024	4	2024
DCO - Tactical DCO-Infrastructure -TDI- RDP INC 2	3	2024	3	2024

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 5	**R-1 Program Element (Number/Name)** PE 0605041A **/** *Defensive CYBER Tool Development*	**Project (Number/Name)** EV5 **/** *Defensive CYBER Operations*

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
DCO - Cyberspace Analytics Big Data Platform	1	2017	3	2018
DCO - Cyberspace Analytics Micro Analytics	2	2017	3	2019
DCO - Cyberspace Analytics Continuous Monitoring	4	2017	2	2018
DCO - Cyberspace Analytics Program of Record - Contract Award	1	2019	1	2019
DCO - Cyberspace Analytics Behavioral Patterns - Contract Award	2	2020	2	2020
DCO - Cyberspace Analytics Threat Trends - Contract Award	1	2020	1	2020
DCO - Cyberspace Analytics Prime Contract - Contract Award	3	2020	3	2020
DCO - Cyberspace Analytics RDP Approval	3	2018	3	2018
DCO - Mission Planning Program of Record - Contract Award	1	2019	1	2019
DCO - Mission Planning RDP Approval	3	2018	3	2018
DCO - Mission Planning Prototype	1	2018	2	2019
DCO - Tools Suite Integration	1	2019	4	2023
DCO - Garrison DCO Platform Capability Enhancements	2	2019	4	2023
DCO - Forensics and Malware RDP Approval	1	2019	1	2019
DCO - User Activity Monitoring RDP Approval	1	2019	1	2019
DCO - Deployable DCO System Prototype - Contract Award	1	2020	1	2020
DCO - Garrison DCO Platform Prototype - Contract Award	1	2019	1	2019