Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army											Date: February 2020	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 8: *Software and Digital Technology Pilot Programs*					R-1 Program Element (Number/Name) PE 0608041A *I Defensive CYBER - Software Prototype Development*							
COST ($ in Millions)	**Prior Years**	**FY 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
Total Program Element	-	0.000	0.000	46.445	-	46.445	115.064	109.787	105.851	92.632	0.000	469.779
CD1: *Defensive Cyber - Software Prototype Devel*	-	0.000	0.000	46.445	-	46.445	115.064	109.787	105.851	92.632	0.000	469.779

Note

Defensive Cyber Operations (DCO) programs were selected as a candidate for the BA8 Software RDT&E Appropriation Pilot Program in FY 2021. These efforts are a continuation and transfer from RDTE PE 0605041A EV5, OPA PE 0128B63000, and OMA SAG 151251. Cyber Situational Understanding (SU), DCO Development Environment (DCODE) (formerly Forge), and non-software Army Cyber Command (ARCYBER) Rapid Cyber Prototyping are not part of the Software Pilot and remain within RDTE PE 0605041A. In addition, Garrison Defensive Platforms (GDP) and Deployable DCO Systems (DDS) remain within OPA PE 0128B63000.

A. Mission Description and Budget Item Justification

Defensive Cyber Operations (DCO) supports the Army Network Modernization Strategy Line of Effort (LOE) Key Enabler for Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy. The DCO budget line includes funding for Program Executive Office Command Control and Communications - Tactical (PEO C3T) Tactical DCO Infrastructure (TDI); Program Executive Office Enterprise Information Systems (PEO EIS) Defensive Cyber Operations; and Army Cyber Command (ARCYBER) Rapid Cyber Prototyping.

Platforms/Levels:
* DCO - Tactical DCO Infrastructure (TDI) - (PEO C3T) - Tactical/Command Post Level
* DCO - Cyberspace Analytics - (PEO EIS) - (Gabriel Nimbus) - Strategic Level (Army Cyberspace Operations and Integration Center (ACOIC))

Defensive Cyber Tools and Analytics:
* DCO - Cyberspace Analytics - (PEO EIS) - Strategic Level (ACOIC)
* DCO - Mission Planning - (PEO EIS) - Strategic Level
* DCO - Tools Suite - (PEO EIS) - Garrison/Tactical Level
* DCO - User Activity Monitoring - (PEO EIS) - Strategic Level
* DCO - Forensics and Malware Analysis - (PEO EIS) - Garrison/Tactical Level
* DCO - Threat Emulation - (PEO EIS) - Strategic Level (Training)

- Tactical DCO Infrastructure (TDI) is a software-only program, which consists of pre-configured DCO tools residing on the Tactical Server Infrastructure (TSI). The TDI capability will reside within the Command Post at echelon Corps through Brigade for both organic Cyber Network Defenders as well as remote access by Cyber Protection teams (CPT) to support defense of the Tactical Network.

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army	Date: February 2020
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 8: *Software and Digital Technology Pilot Programs*	**R-1 Program Element (Number/Name)** PE 0608041A *I Defensive CYBER - Software Prototype Development*

- Defensive Cyber Operations (DCO) consists of platform and software programs which are key elements of the DCO Maneuver Baseline infrastructure, platform, and tools. The employment of defensive capabilities creates specific effects in cyberspace through actions that allow commanders to achieve the following objectives: deter, destroy, and defeat enemy offensive cyberspace operations; gain time; economy of force; control key terrain; protect tasked critical assets and infrastructure; and develop intelligence. DCO supports the Army Cyber Command (ARCYBER), ACOIC, (5) Regional Cyber Centers (RCCs), Cyber Warfare Battalion (CWB), Multi-Domain Task Force (MDTF), Cyber Protection Brigade (CPB), and (41) Cyber Protection Teams (CPTs) in COMPO 1/2/3.

- ARCYBER Rapid Cyber Prototyping provides software based capabilities that can quickly respond to emerging cyber threats and keep up with threat technology. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in tactics techniques and procedures (TTPs), and trends of adversarial activity. These are separate and distinct from DCO programs identified and are used to rapidly address a network threat/ vulnerability.

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	0.000	0.000	0.000	-	0.000
Current President's Budget	0.000	0.000	46.445	-	46.445
Total Adjustments	0.000	0.000	46.445	-	46.445
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	46.445	-	46.445

Change Summary Explanation

FY21 funding in the amount of $46.445 million was realigned to the Software RDTE Appropriation Pilot Program.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 8	R-1 Program Element (Number/Name) PE 0608041A / *Defensive CYBER - Software Prototype Development*	Project (Number/Name) CD1 / *Defensive Cyber - Software Prototype Devel*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
CD1: *Defensive Cyber - Software Prototype Devel*	-	0.000	0.000	46.445	-	46.445	115.064	109.787	105.851	92.632	0.000	469.779

Note

Defensive Cyber Operations (DCO) programs were selected as a candidate for the BA8 Software RDT&E Appropriation Pilot Program in FY 2021. These efforts are a continuation and transfer from RDTE PE 0605041A EV5, OPA PE 0128B63000, and OMA SAG 151251. Cyber Situational Understanding (SU), DCO Development Environment (DCODE) (formerly Forge), and non-software Army Cyber Command (ARCYBER) Rapid Cyber Prototyping are not part of the Software Pilot and remain within RDTE PE 0605041A. In addition, Garrison Defensive Platforms (GDP) and Deployable DCO Systems (DDS) remain within OPA PE 0128B63000.

A. Mission Description and Budget Item Justification

Defensive Cyber Operations (DCO) supports the Army Network Modernization Strategy Line of Effort (LOE) Key Enabler for Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy. The DCO budget line includes funding for Program Executive Office Command Control and Communications - Tactical (PEO C3T) Tactical DCO Infrastructure (TDI); Program Executive Office Enterprise Information Systems (PEO EIS) Defensive Cyber Operations; and Army Cyber Command (ARCYBER) Rapid Cyber Prototyping.

Platforms/Levels:
* DCO - Tactical DCO Infrastructure (TDI) - (PEO C3T) - Tactical/Command Post Level
* DCO - Cyberspace Analytics - (PEO EIS) - (Gabriel Nimbus) - Strategic Level (Army Cyberspace Operations and Integration Center (ACOIC))

Defensive Cyber Tools and Analytics:
* DCO - Cyberspace Analytics - (PEO EIS) - Strategic Level (ACOIC)
* DCO - Mission Planning - (PEO EIS) - Strategic Level
* DCO - Tools Suite - (PEO EIS) - Garrison/Tactical Level
* DCO - User Activity Monitoring - (PEO EIS) - Strategic Level
* DCO - Forensics and Malware Analysis - (PEO EIS) - Garrison/Tactical Level
* DCO - Threat Emulation - (PEO EIS) - Strategic Level (Training)

- Tactical DCO Infrastructure (TDI) is a software-only program, which consists of pre-configured DCO tools residing on the Tactical Server Infrastructure (TSI). The TDI capability will reside within the Command Post at echelon Corps through Brigade for both organic Cyber Network Defenders as well as remote access by Cyber Protection teams (CPT) to support defense of the Tactical Network.

- Defensive Cyber Operations (DCO) consists of platform and software programs which are key elements of the DCO Maneuver Baseline infrastructure, platform, and tools. The employment of defensive capabilities creates specific effects in cyberspace through actions that allow commanders to achieve the following objectives:

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

deter, destroy, and defeat enemy offensive cyberspace operations; gain time; economy of force; control key terrain; protect tasked critical assets and infrastructure; and develop intelligence. DCO supports the Army Cyber Command (ARCYBER), ACOIC, (5) Regional Cyber Centers (RCCs), Cyber Warfare Battalion (CWB), Multi-Domain Task Force (MDTF), Cyber Protection Brigade (CPB), and (41) Cyber Protection Teams (CPTs) in COMPO 1/2/3.

- ARCYBER Rapid Cyber Prototyping provides software based capabilities that can quickly respond to emerging cyber threats and keep up with threat technology. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in tactics techniques and procedures (TTPs), and trends of adversarial activity. These are separate and distinct from DCO programs identified and are used to rapidly address a network threat/ vulnerability.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Defensive Cyber Operations (DCO) - Tactical DCO Infrastructure (TDI) (PEO C3T)	-	-	5.000
Description: DCO Tactical DCO Infrastructure is a software-only program which consists of pre-configured DCO Tools on the Tactical Server Infrastructure (TSI) residing within the Command Post, at Brigade through Corps, for both organic Cyber Network Defenders as well as remote access by Cyber Protection Teams (CPTs) to support defense of the tactical network. ***FY 2021 Plans:*** FY 2021 funding supports development engineering, integration and testing of Capability Drop 2 (CD 2). CD 2 will integrate the enhanced DCO tool suite that will leverage machine learning and expand the data collection beyond the command post to the extended tactical network. Finalize integration of current DCO remote operations capability to facilitate timely escalation of remote incident response. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.			
Title: Defensive Cyber Operations - Cyber Analytics (PEO EIS)	-	-	9.490
Description: DCO Cyberspace Analytics Big Data Platform (BDP) is a scalable software based capability hosted in the cloud, called Gabriel Nimbus (GN), which offers interfaces and visualization accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities meant to discover the presence of advanced or sophisticated cyber threats and vulnerabilities. ***FY 2021 Plans:*** FY 2021 funding supports software and modification to BDP/GN to include engineering, integration, and testing of capability releases and capability drops. These software upgrades have been approved by Configuration Control Board (CCB) to be included in the Army's BDP which Soldiers are using today. Provides Cross Domain Solution between Network Internet Protocol Router (NIPR), Secret Internet Protocol Router (SIPR), and Joint Worldwide Intelligence Communications Systems (JWICS). Enables separate organizations at multiple echelons to develop mutually supporting cyberspace analytics independently. Enriches			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
and stores data for follow-on correlation and analysis to determine the presence of anomalous network activity and understand the associated impacts. Facilitates the identification of threat trends, behavior patterns, and tactics, techniques, and procedures associated with relevant portions of the designated network. Ingests multitudes of data sources, and turns that data into visual information in order to detect and illuminate adversaries. Key to mission success is the collection of data on our platforms and the integration with GN through the Lower Echelon Analytic Platform (LEAP) which are vital to achieve this vision. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.			
Title: Defensive Cyber Operations (DCO) - Mission Planning (PEO EIS) ***Description:*** DCO Mission Planning (DCOMP) solution acts as the lead application integrator for the Army's Big Data Platform. It is a software application-based, scalable warfighting capability for ACOIC mission and planning at the tactical and strategic levels. ***FY 2021 Plans:*** FY 2021 funding supports development engineering, integration, and testing of three capability releases (software upgrades). Delivers mission command and planning at all levels supporting Cyber Defense Forces. Creates a DCO mission execution framework by utilizing PhalanX to collaborate, understand, plan, and manage DCO missions in real-time. Provides on-demand capabilities available within capability libraries matched to the overall effects requested by Commanders. Offers shared situational awareness amongst cyberspace defenders about their missions and area of operations. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.	-	-	4.700
Title: Defensive Cyber Operations (DCO) - Tools Suite (PEO EIS) ***Description:*** DCO Tools Suite is a flexible and dynamic software based suite of warfighting capabilities that enables CPTs, RCCs, and in some cases local defenders to perform DCO and cybersecurity actions. DCO tools consists of prepositioned and tailorable software packages that are integrated and available at all echelons to support or directly cause effects through the execution of Cyber Mission Force and cyberspace workforce tasks. They are executed or managed within a DCO platform. ***FY 2021 Plans:*** FY 2021 funding supports procurement, development engineering, integration, and testing of DCO Tools Suite v5.0 and v6.0 (perpetual, subscription, and open source tools like Redhat, Redseal, Cobalt Strike, Splunk, Carbon Black, Forescout, Aspera, and Emerging Threat Pro). Employs defeat mechanisms to destroy, dislocate, disintegrate and isolate cyberspace threats/ vulnerabilities. Conducts full range of military operations and ensures use of key terrain in cyberspace. Gains and maintains the	-	-	17.900

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
advantage and places adversaries at disadvantage in increasingly congested/contested space, cyberspace, and electromagnetic spectrum. Without these tools cyber defenders will not be able to conduct Network Mapping, Event Correlation, Threat Emulation, Endpoint Security, Massive Data Transference, Terrain Analysis, Continuous Monitoring, Intel Support, and DEVSECOPS. Threat Deception (formerly known as Counter Infiltration) has been added as a Capability Drop which identifies and block infiltration attempts. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from OPA PE 0128B63000 and OMA SAG 151251. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.			
Title: Defensive Cyber Operations (DCO) - User Activity Monitoring (PEO EIS) ***Description:*** DCO User Activity Monitoring is the primary capability within the Army's overall Insider Threat program. UAM is primarily a software-based, scalable solution (some hardware in the on-premise solution) that proactively identifies and mitigates internal risks associated with the theft or misuse of critical, mission essential data. It utilizes an integrated approach with a centralized UAM cell sending data to a core Insider Threat Hub. ***FY 2021 Plans:*** FY 2021 funding supports development engineering, integration, and testing of two capability drops (on-premise solution). Provides protection against insider threat through the deployment of capability in defense of our most critical networks. Proactively identifies and mitigates internal risks associated with the theft or misuse of critical, mission essential data. Assists with the establishment of the Army's Insider Threat (InT) Protection Program that utilizes full-spectrum solutions to assess, deter, deny, defend, defeat, and evolve against the insider threat. Facilitates the ability to identify insiders threats based on policy violations, as well as the capturing of certain risk behaviors that rate the likelihood of an incident caused by a trusted insider. Integrates behavioral based analysis capability through the use of GN. The Army will implement UAM for all Soldiers, civilians, and contractors with access to JWICS and SIPRNet. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.	-	-	2.550
Title: Defensive Cyber Operations (DCO) - Forensics and Malware Analysis (PEO EIS) ***Description:*** DCO Forensics and Malware Analysis capability is a software/hardware based solution enabling global, regional, and local cyberspace defenders to perform forensics either remotely or locally. Forensics is evidence related and Malware capabilities provides a sandboxlike, virtual environment that allows for the conduct of real-time, automated and dynamic malware decomposition and behavior analysis. Forensics gives cyberspace defenders the ability to collect, process, search, and analyze	-	-	3.020

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
evidence from portable electronic devices, removable media, system hard drives, and random access memory. This process rapidly triages an incident and place the impacted system(s) back in service. ***FY 2021 Plans:*** FY 2021 funding supports development engineering, integration, and testing of capability drops for initial operating capability (IOC) in 2Q21. Deploys forensics capability within each theater of operation enabling the RCC and CPTs to conduct live forensics on critical assets. Provides capability to collect and examine data either remotely or locally using a repeatable and defensible process to include (1) triage - ability to quickly view and conduct comprehensive searching on potential evidence; (2) evidence acquisition - provides centralized-node enterprise in which analysts can preview, acquire, and analyze evidence remotely and locally; (3) data processing - provides processing capabilities that can automate the preparation of evidence; (4) analysis - allows a semi-automated capability to analyze file systems, compressed files, timelines, web histories, recycle bins, memory, disks, logs, registries, and other artifacts; and (5) reporting - provides flexible reporting framework that empowers analysts to tailor their case report. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from OPA PE 0128B63000. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.			
Title: Defensive Cyber Operations (DCO) - Threat Emulation (PEO EIS) ***Description:*** DCO Threat Emulation capability is a software based suite of tools used to gain access to evaluated networks and through multi-vectors of unknown, partially known, or known access methods. Threat Emulation will enable the implementation of real world threat tactics, techniques, and procedures (TTPs) against risk areas such as web services, endpoints, passwords and identities, phishing and social engineering, mobile devices, and wired/wireless network systems in order to reveal critical security exposures. ***FY 2021 Plans:*** FY 2021 funding supports development engineering, integration, and testing. It provides software based capability that will allow CPTs to not only asses the ability of systems to withstand an advance persistent threat actor attack by evaluating the people and processes. Enables the implementation of real world threat TTPs against risk areas such as web services, endpoints, passwords and identities, phishing and social engineering, mobile devices, and wired/wireless network systems in order to reveal critical security exposures. Exists within a contemporary operational environment consisting of a collective set of conditions, derived from a composite of actual worldwide conditions that pose realistic challenges for training, leader development, and capabilities development. ***FY 2020 to FY 2021 Increase/Decrease Statement:***	-	-	1.600

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.			
Title: Defensive Cyber Operations (DCO) - Management Services (PEO EIS) ***Description:*** Program management services consists of System Engineering and Technical Assistance (SETA) contractors and government/contract matrix support from Software Engineering Center (SEC), Information Systems Engineering Command (ISEC), and Army Test and Evaluation Command (ATEC) for development engineering, integration, and testing of software based DCO capabilities. ***FY 2021 Plans:*** FY 2021 funding provides continued program management services and support. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from RDTE PE 0605041A EV5. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.	-	-	1.720
Title: Defensive Cyber Operations (DCO) - Rapid Cyber Prototyping (ARCYBER) ***Description:*** ARCYBER Rapid Cyber Prototyping provides software based capabilities that can quickly respond to emerging cyber threats and keep up with threat technology. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in TTPs, and trends of adversarial activity. These are separate and distinct from DCO programs identified and are used to rapidly address a network threat/vulnerability. ***FY 2021 Plans:*** FY 2021 funding supports the procurement and modification of software based Emerging Threat Response Development tools. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** These efforts are a continuation of and transfer from OPA PE 0128B63000. FY 2021 is the first year of the BA8 Software RDT&E Appropriation Pilot Program.	-	-	0.465
Accomplishments/Planned Programs Subtotals	-	-	46.445

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

- Realigned $25.060 million FY21 RDTE from PE 0605041A to Software RDTE Appropriation Pilot Program:
* Tactical DCO Infrastructure $5.000 million

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

C. Other Program Funding Summary ($ in Millions)

* Cyber Analytics $9.490 million
* User Activity Monitoring $2.550 million
* Mission Planning $4.700 million
* Threat Emulation $1.600 million
* DCO Management Services $1.720 million

- Realigned $16.593 million FY21 OPA from PE 0128B63000 to Software RDTE Appropriation Pilot Program:
* DCO Tools Suite $13.108 million
* Forensics and Malware $3.020 million
* ARCYBER Rapid Cyber Prototyping $0.465 million

- Realigned $4.792 million FY21 OMA from SAG 151251 to Software RDTE Appropriation Pilot Program:
* DCO Tools Suite $4.792 million

D. Acquisition Strategy

The DCO Information System Capabilities Development Document (IS ICD) was approved on 19 Dec 17 by the Army Requirements Oversight Council (AROC). DCO programs are under an IT Box construct with five year term (FY18-22) which aligns with current Requirements Definition Package (RDP).

The Milestone Decision Authority (MDA), approved the Materiel Development Decision (MDD) on 13 Apr 18, designating Tactical DCO Infrastructure (TDI) as an ACAT III program. The TDI program's RDP was approved on 8 Nov 18 by the Army Requirement Board (ARB). Under subsequent reviews, the MDA approved a tailored defense unique software intensive acquisition approach for TDI. To support this agile acquisition approach, the TDI program office will develop and deploy pre-configured software in a series of capability drops in order to deliver full functional values of the RDP that align with DCO priorities. The TDI program had a Full Deployment Decision (FDD) of TDI's initial capability approved by the MDA on Sep 19, which allowed the program to achieve IOC Oct 19. TDI is hosted on the Tactical Server Infrastructure (TSI) and will be fielded by the CPCE/TSI program in accordance with their fielding schedule. Execution of the TDI program will be a combination of government entities and commercial vendors.

The ARB approved Cyber Analytics and DCO Tool Suite RDPs on 24 Apr 18; Mission Planning on 26 Jun 18; and User Activity Monitoring and Forensics and Malware on 16 Oct 18. The MDA designated these as ACAT IV programs. Under subsequent reviews, the MDA approved agile acquisition approach to develop and deliver pre-configured software in a series of releases and capability drops in order to deliver full functional values of the RDP that align with DCO priorities. DCO programs utilize standard and 874 agile pilot evolutionary acquisition processes (30-90 rapid acquisition approach). DCO continually delivers new technologies and capabilities as a prototype and fields updated capabilities. DCO contract strategy utilizes multiple existing contracts vehicles to include Other Transactional Authority (OTA), Federal Acquisition Regulation (FAR)-based, Blanket Purchase Agreement (BPA), and Basic Ordering Agreement (BOA).

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO -Tactical DCO Infrastructure (TDI) (PEO C3T)	C/FFP	CACI : Aberdeen Proving Ground, (APG) MD	-	-		-		0.378		-		0.378	0.000	0.378	-
DCO - Management Services (PEO EIS)	SS/TBD	Various : Various	-	-		-		1.720		-		1.720	0.000	1.720	-
		Subtotal	-	-		-		2.098		-		2.098	0.000	2.098	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical DCO Infraastructure (TDI) (PEO C3T)	C/CPFF	Parsons and CACI : ACC-RI: IL	-	-		-		3.468		-		3.468	0.000	3.468	-
DCO - Cyber Analytics (PEO EIS)	C/FFP	Army Contracting Command - Rock Island (ACC-RI) : Rock Island, IL	-	-		-		9.490		-		9.490	0.000	9.490	-
DCO - Tools Suite (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		17.900		-		17.900	0.000	17.900	-
DCO - Mission Planning (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		4.700		-		4.700	0.000	4.700	-
DCO - User Activity Monitoring (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		2.550		-		2.550	0.000	2.550	-
DCO - Forensics and Malware (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		3.020		-		3.020	0.000	3.020	-
DCO - Threat Emulation (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		1.600		-		1.600	0.000	1.600	-
DCO - Rapid Cyber Prototyping (ARCYBER)	C/FFP	ACC-RI : Rock Island, IL	-	-		-		0.465		-		0.465	0.000	0.465	-
		Subtotal	-	-		-		43.193		-		43.193	0.000	43.193	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 8	R-1 Program Element (Number/Name) PE 0608041A / *Defensive CYBER - Software Prototype Development*	Project (Number/Name) CD1 / *Defensive Cyber - Software Prototype Devel*	

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical Development Infrastructure (TDI) (PEO C3T)	MIPR	DLA : Philadelphia, PA	-	-		-		0.115		-		0.115	0.000	0.115	-
		Subtotal	-	-		-		0.115		-		0.115	0.000	0.115	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical Development Infrastructure (TDI) (PEO C3T)	MIPR	ATEC : Aberdeen Proving Ground, (APG) MD	-	-		-		1.039		-		1.039	0.000	1.039	-
		Subtotal	-	-		-		1.039		-		1.039	0.000	1.039	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	-		0.000		46.445		-		46.445	0.000	46.445	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

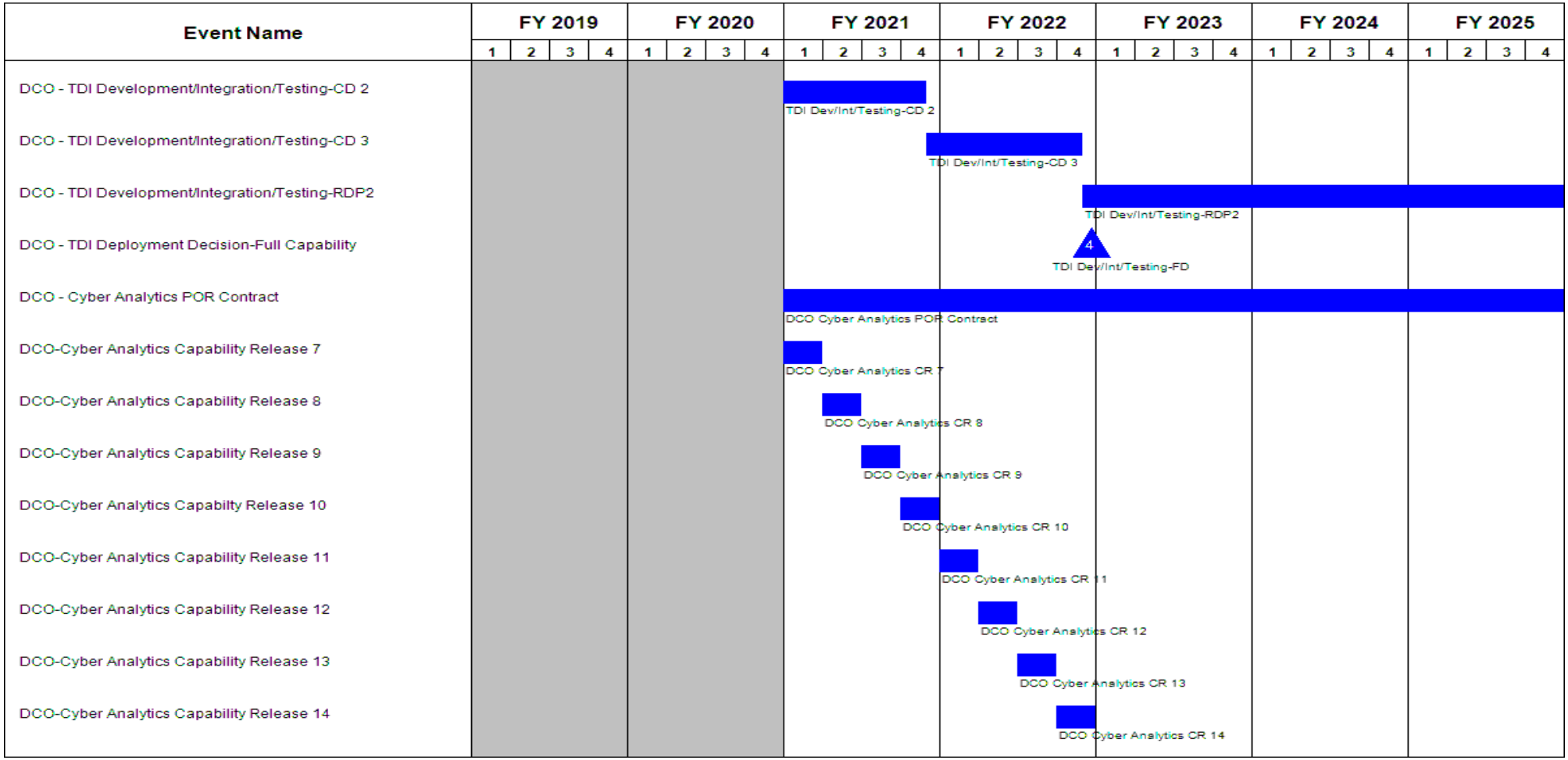


Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

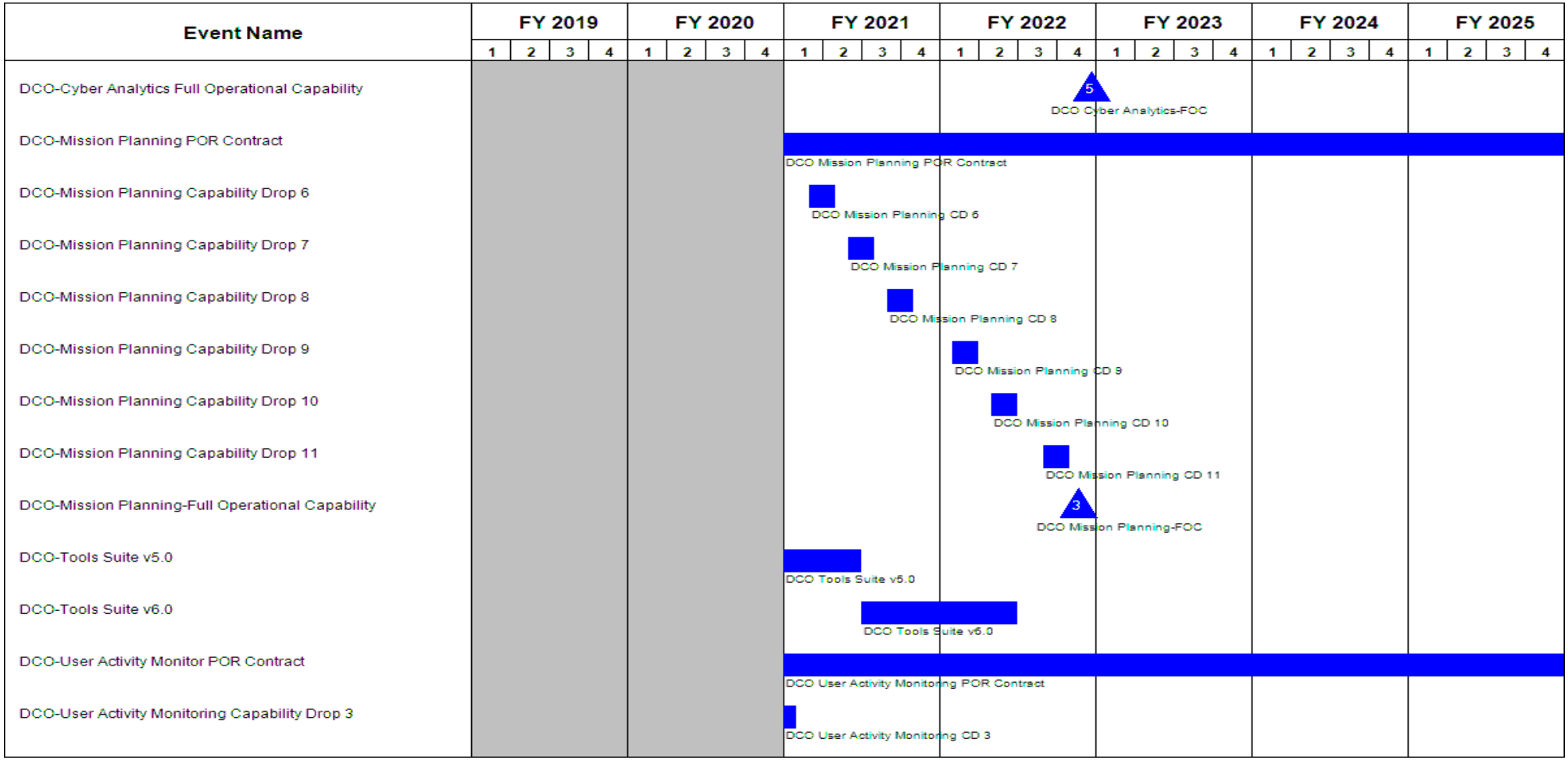


Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

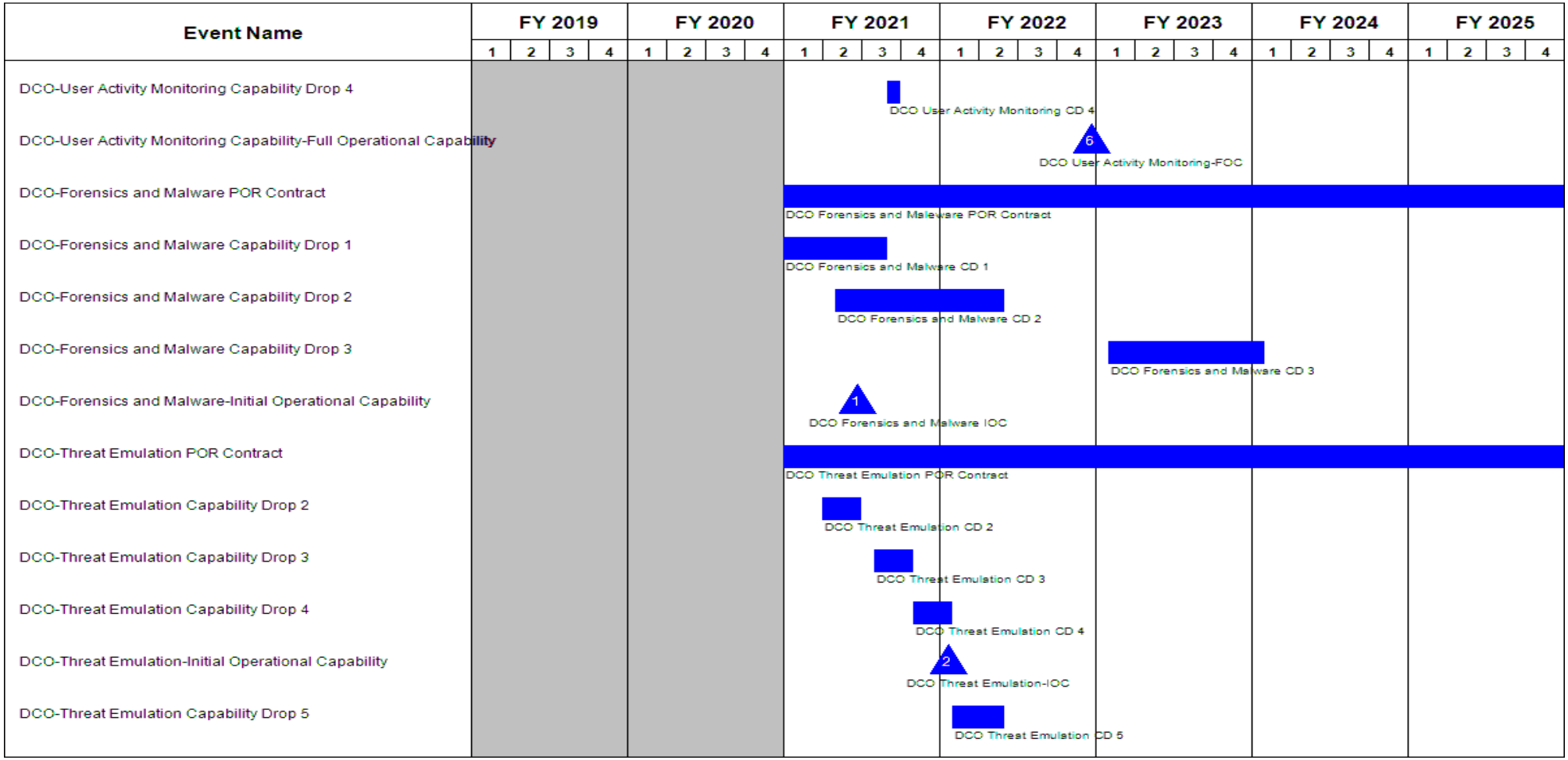
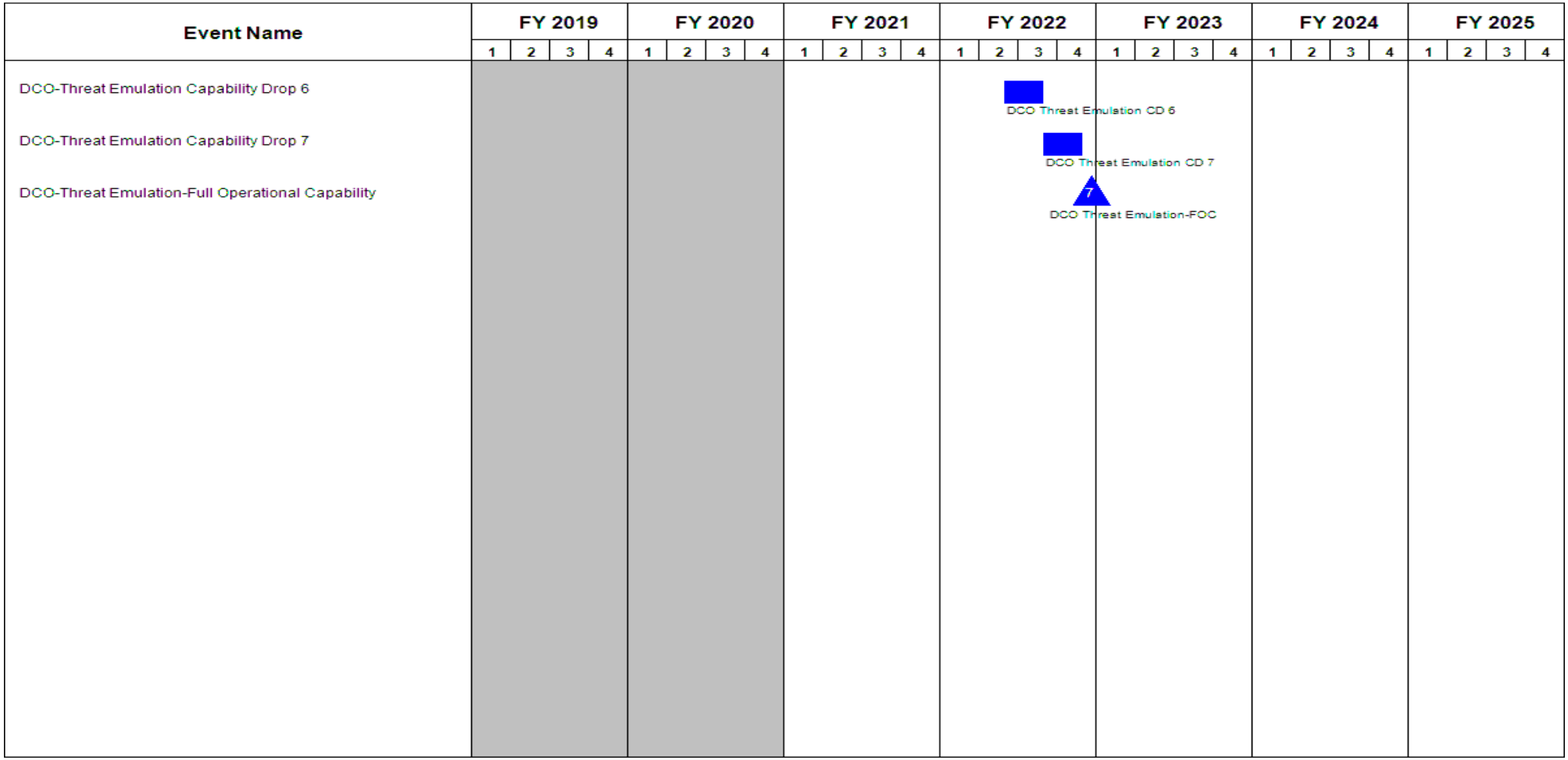


Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*



Note

Tactical DCO Infrastructure: Full Deployment is defined as when TDI has completed the development and testing of the last capability drop within the IT Box (reaching full functional values of the RDP) and has transferred the capability to the CPCE/TSI program to commence fielding.

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

Current DCO IT box ends in FY22. TCM is working a new DCO IS ICD to align with a new IT Box construct for FY23-27.

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
DCO - TDI Development/Integration/Testing-CD 2	1	2021	4	2021
DCO - TDI Development/Integration/Testing-CD 3	4	2021	4	2022
DCO - TDI Development/Integration/Testing-RDP2	4	2022	4	2025
DCO - TDI Deployment Decision-Full Capability	4	2022	4	2022
DCO - Cyber Analytics POR Contract	1	2021	4	2025
DCO-Cyber Analytics Capability Release 7	1	2021	1	2021
DCO-Cyber Analytics Capability Release 8	2	2021	2	2021
DCO-Cyber Analytics Capability Release 9	3	2021	3	2021
DCO-Cyber Analytics Capabilty Release 10	4	2021	4	2021
DCO-Cyber Analytics Capability Release 11	1	2022	1	2022
DCO-Cyber Analytics Capability Release 12	2	2022	2	2022
DCO-Cyber Analytics Capability Release 13	3	2022	3	2022
DCO-Cyber Analytics Capability Release 14	4	2022	4	2022
DCO-Cyber Analytics Full Operational Capability	4	2022	4	2022
DCO-Mission Planning POR Contract	1	2021	4	2025
DCO-Mission Planning Capability Drop 6	1	2021	2	2021
DCO-Mission Planning Capability Drop 7	2	2021	3	2021
DCO-Mission Planning Capability Drop 8	3	2021	4	2021
DCO-Mission Planning Capability Drop 9	1	2022	1	2022
DCO-Mission Planning Capability Drop 10	2	2022	2	2022
DCO-Mission Planning Capability Drop 11	3	2022	4	2022
DCO-Mission Planning-Full Operational Capability	4	2022	4	2022

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
DCO-Tools Suite v5.0	1	2021	2	2021
DCO-Tools Suite v6.0	3	2021	2	2022
DCO-User Activity Monitor POR Contract	1	2021	4	2025
DCO-User Activity Monitoring Capability Drop 3	1	2021	1	2021
DCO-User Activity Monitoring Capability Drop 4	3	2021	3	2021
DCO-User Activity Monitoring Capability-Full Operational Capability	4	2022	4	2022
DCO-Forensics and Malware POR Contract	1	2021	4	2025
DCO-Forensics and Malware Capability Drop 1	1	2021	3	2021
DCO-Forensics and Malware Capability Drop 2	2	2021	2	2022
DCO-Forensics and Malware Capability Drop 3	1	2023	1	2024
DCO-Forensics and Malware-Initial Operational Capability	2	2021	2	2021
DCO-Threat Emulation POR Contract	1	2021	4	2025
DCO-Threat Emulation Capability Drop 2	2	2021	2	2021
DCO-Threat Emulation Capability Drop 3	3	2021	4	2021
DCO-Threat Emulation Capability Drop 4	4	2021	1	2022
DCO-Threat Emulation-Initial Operational Capability	1	2022	1	2022
DCO-Threat Emulation Capability Drop 5	1	2022	2	2022
DCO-Threat Emulation Capability Drop 6	2	2022	3	2022
DCO-Threat Emulation Capability Drop 7	3	2022	4	2022
DCO-Threat Emulation-Full Operational Capability	4	2022	4	2022

Note

TDI full deployment is defined when programs have completed the development and testing of the last capability drop within the IT Box (reaching full functional values of the RDP) and has transferred the capability to the CPCE/TSI program to commence fielding.

DCO is capability owner and full operational capability is defined when programs have completed the development and testing of the last capability drop within the IT Box (reaching full functional values of the RDP).

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

Current DCO IT box ends in FY22. Army Capabilities Manager (ACM, formerly TRADOC Capability Manager (TCM)) is working a new DCO IS ICD to align with a new IT Box construct for FY23-27.