Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army	Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
Total Program Element	-	-	56.706	118.811	-	118.811	-	-	-	-	-	-
CD1: *Defensive Cyber - Software Prototype Devel*	-	-	56.706	118.811	-	118.811	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

Defensive Cyber Operations (DCO) is the only Army program selected for the BA8 Software Pilot Program (PE 0608041A) starting in Fiscal Year (FY) 2021. The program realigned $90.340 million FY 2022 Research, Development, Test, and Evaluation (RDTE) from PE 0605041A EV5 and $28.471 million FY 2022 Other Procurement Army (OPA) from PE 0128B63000 to BA8 Software Pilot Program PE 0608041A CD1.

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.

Defensive Cyber Operations (DCO) and Tactical DCO Infrastructure (TDI) support the Army Network Modernization Strategy Line of Effort (LOE) 1, Key Enabler for Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy.

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)
* DCO - DCO Development Environment (DCODE) - (PEO EIS)
* DCO - Army Cyber Command (ARCYBER) Rapid Cyber Prototyping

- 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 2022 Army	Date: May 2021
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; while supporting Multi-Domain operations. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in the operational information environment and/or trends of adversarial activity; which drive CONOP and TTP modifications. These are separate and distinct from DCO programmed efforts already funded or budgeted for by PM DCO and are used to rapidly address a network threat/vulnerability.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	0.000	46.445	115.064	-	115.064
Current President's Budget	0.000	56.706	118.811	-	118.811
Total Adjustments	0.000	10.261	3.747	-	3.747
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-1.739			
• Congressional Rescissions	-	-			
• Congressional Adds	-	12.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	3.747	-	3.747

Change Summary Explanation

FY 2021 Funding in the amount of $10.261 million increased to the Defensive Cyber program, cited from $12.000 million transferred from FY 2021 OPA PE 0128B63000 to BA8 Software Pilot Program PE 0608041A CD1, and $1.739 million decrement due to Tool Suite delays.

FY 2022 Funding in the amount of $3.747 million increased to the Defensive Cyber program, cited from $4.779 million transferred from FY 2022 RDTE PE 0605041A EV5, and $1.032 million decrement due to Army's reprioritization.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
CD1: *Defensive Cyber - Software Prototype Devel*	-	-	56.706	118.811	-	118.811	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Defensive Cyber Operations (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.

Defensive Cyber Operations (DCO) and Tactical DCO Infrastructure (TDI) support the Army Network Modernization Strategy Line of Effort (LOE) 1, Key Enabler for Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy.

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)
* DCO - DCO Development Environment (DCODE) - (PEO EIS)
* DCO - Army Cyber Command (ARCYBER) Rapid Cyber Prototyping

- 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: deter, destroy, and defeat enemy offensive cyberspace operations; gain time; economy of force; control key terrain; protect tasked critical assets and infrastructure; and

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

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; while supporting Multi-Domain operations. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in the operational information environment and/or trends of adversarial activity; which drive CONOP and Tactics Techniques and Procedures (TTP) modifications. These are separate and distinct from DCO programmed efforts already funded or budgeted for by PM DCO and are used to rapidly address a network threat/vulnerability.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Defensive Cyber Operations (DCO) - Tactical DCO Infrastructure (TDI) (PEO C3T)	-	5.000	5.545
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 RDTE Plans: $5.000M 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 2022 Plans:*** FY 2022 RDTE Plans: $5.545M FY 2022 funding supports development engineering, integration, testing, training development and program management to complete the last capability within the current IT box, CD3. CD3 will integrate the enhanced DCO tool suite that will enable broader data collection and data aggregation (including existing logs from other PoRs), and the ability for WiFi and 4G connection monitoring in support of TDI Full Deployment 4QTR FY 2022. PEO C3T will execute these funds. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding increase will provide additional engineering and program management to support completion/Full Deployment of the current IT Box (which plans to be renewed).			
Title: Defensive Cyber Operations - Cyber Analytics (PEO EIS)	-	16.187	35.800

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022

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:
In 2020, significantly expanded the Army?s BDP on the Non-Classified Internet Protocol Router (NIPR) cloud, increasing storage from (6.7) petabytes (PB) to (14) PB. Also, initiated the Secret Internet Protocol Router (SIPR) cloud through a Military Operations Area (MOA) with the National Geospatial Intelligence Agency (NGA) which also provides support to Army Vantage and General Fund Enterprise Business System (GFEBS-SA). In addition, GN was deployed to the Joint Worldwide Intelligence Communications Systems (JWICS) environment by leveraging the Army Military Intelligence Commercial Cloud Services Provider (AC2SP) from the National Ground Intelligence Center (NGIC). Access to Amazon Web Services (AWS) SIPR and JWICS environments in the cloud are rare for organizations outside the Intelligence Community.

FY 2021 RDTE Plans: $13.187M
FY 2021 funding supports software and modification to BDP/GN to include engineering, integration, and testing of Capability Releases that support seven main areas of needed capability: First is Multi-Domain, Second is Battlespace Awareness, Third is Intelligence Integration, Fourth is DCO/Cybersecurity, Fifth is Machine Learning/AI, Sixth is Cyber IT/OT (SCADA), and Seventh is DevOps/Lower Echelon Analytic Platform (LEAP). 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 NIPR, SIPR, and JWICS. Enables separate organizations at multiple echelons to develop mutually supporting cyberspace analytics independently. Enriches 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 LEAP.

FY 2021 OMA Plans: $3.000M
FY 2021 funding supports GN cloud hosting infrastructure of (3) PB SIPR.

FY 2022 Plans:
FY 2022 RDTE Plans: $12.300M
FY 2022 funding supports software and modification to BDP/GN to include engineering, integration, cybersecurity, and testing of capability releases (11) through (14) leading to Full Operational Capability (FOC). It is anticipated that Cyber Analytics will achieve

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
FOC in 4Q FY 2022. Cyber Analytics capability will be installed and operational on designated infrastructure at the regional and local level to ingest, process, and store corresponding data. FY 2022 OMA Plans: $23.500M FY 2022 funding supports all hosting costs for (10) PB of NIPR that is needed from a strategic perspective to help prevent possible future cyber attacks, (3) PB of SIPR, and (3) PB of JWICS ((2) PB for Cyber Analytics and (1) PB for User Activity Monitoring). Cloud hosting size must be large enough to efficiently ingest all of the data feeds, and any PB increase will also increase the costs of the management tool and managed professional services. FY 2022 funding also supports software and modification to BDP/GN to include engineering, integration, cybersecurity, and testing of capability releases (11) through (14) leading to Full Operational Capability (FOC). It is anticipated that Cyber Analytics will achieve FOC in 4Q FY 2022. Cyber Analytics capability will be installed and operational on designated infrastructure at the regional and local level to ingest, process, and store corresponding data. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding transferred from RDTE PE 0605041A EV5. The funding increase will support all cloud hosting costs of NIPR/ SIPR/JWICS, along with software and modification to BDP/GN to include engineering, integration, cybersecurity and testing of capability releases leading to FOC in 4Q FY 2022. Specifically, installing capabilities on all designated infrastructure at regional DCO levels to ingest, process, and store data. Additionally, network operators / cyberspace defenders at all levels will have required access to conduct missions.			
Title: Defensive Cyber Operations (DCO) - Mission Planning (PEO EIS) ***Description:*** DCO Mission Planning (DCOMP) Solution is a software solution that facilitates situational awareness and understanding, workflow for order execution, and capabilities that bridge the gap between strategic, operational, and tactical cyberspace operators which enable targeted decision support products on existing DCO systems. ***FY 2021 Plans:*** FY 2021 RDTE Plans: $1.100M FY 2021 funding supports development engineering, integration, and testing of one capability release. Delivers mission command and planning at all levels supporting Cyber Defense Forces. Creates a DCO mission execution framework by utilizing the DCOMP Solution to collaborate, understand, plan, and manage DCO missions in real-time. Provides on-demand capabilities within the Army's Big Data Platform (Version 4.1). Offers shared situational awareness amongst cyberspace defenders about their missions and areas of operation. Due to needed re-engineering of the DCOMP Solution to accommodate for a change in the BDP version, the IOC was moved from 4Q FY 2020 to 3Q FY 2021. ***FY 2022 Plans:***	-	1.100	9.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2022 RDTE Plans: $9.000M FY 2022 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 the DCOMP Solution to collaborate, understand, plan, and manage DCO missions in real-time. Offers a shared situational awareness amongst cyberspace defenders about their missions and areas of operation. It is anticipated that Mission Planning will achieve FOC in 4QTR FY 2022. FOC shall be considered attained when DCOMP capabilities are met IAW functional values agreed upon by the capability developer, operational user, program office, and evaluators; FOC additionally requires the DCOMP solution to be capable of autonomously allocating virtual resources and installing DCO tools within the corresponding guest operating systems so that cyberspace defenders can immediately conduct missions upon maneuvering to the supporting infrastructure. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding transferred from RDTE PE 0605041A EV5. The increase in FY 2022 will support development engineering, integration, and testing of three capability releases (software upgrades). These capability releases are critical to reaching FOC by the end of FY 2022. In addition, the DCOMP Solution plans to be transitioned to the JCC2 Program Office at the beginning of FY 2023. Therefore, any requested capabilities from JCC2 that fall within the requirements list will be completed by Defensive Cyber Operations in FY 2022 before the FY 2023 transition.			
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 Cyber Protection Teams (CPTs), Regional Cyber Centers (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 (CMF) and cyberspace workforce tasks. They are executed or managed within a DCO platform. ***FY 2021 Plans:*** FY 2021 OPA Plans: $2.866M FY 2021 funding supports procurement, development engineering, integration, and testing of DCO Tools Suite v3 (perpetual, subscription, and open source tools). 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 advantage and places adversaries at disadvantage in increasingly / 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 violations, as well as the capturing of certain risk behaviors that rate the likelihood of an incident caused by a	-	18.285	26.267

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022

trusted insider. FY 2021 funding supports DCO Hardware Kits increased by (20) DDS and (21) GDP requiring additional tool suite licenses.

FY 2021 OMA Plans: $15.419M
FY 2021 funding supports license renewals and professional services.

FY 2022 Plans:
FY 2022 OPA Plans: $6.867M
FY 2022 funding supports procurement of new tools and renewal of existing tools providing the following capabilities: New capabilities include Network visualization within the cloud, Security Orchestration Automation and Response (SOAR), Single Node Solution (Operating System pilot), and testing of new requirements like Cyberlens a possible Industrial Control System and Supervisory Data Acquisition solution; and Renewals include capabilities like Discovery (Network), Vulnerability Analysis, Command and Control, Threat Emulation, Acquisitions Data, High Speed Data Transport, Endpoint Detection and Recovery (EDR), intel analysis, Continuous Monitoring, Mitigate/Clear/Remediate, Event Correlation, DevSecOps, license renewals, and new equipment training. A new tools suite will be procured every year. Each new tools suite is derived from ARCYBER's annually published requirements and priorities. Tools suites may differ from year to year as some tools are divested, while new tools are added to include any innovations or advances in technology. DCO Tools Suite v4 will begin in FY 2022, and Tools Suite v5 will drop in FY 2023. The users and operators of the tools are the CPTs and Soldiers. The increase in funding will allow the PM to prototype future tool that may be added the tool suite purchase.

FY 2022 OMA Plans: $19.400M
FY 2022 funding support license renewals and professional services.

FY 2021 to FY 2022 Increase/Decrease Statement:
FY 2022 funding transferred from OPA PE 0128B63000. FY 2022 funding increases will support the following: additional testing for Cyberlens software, Single Node Solution (finding a solution to use a smaller deployment footprint of Red Hat), Security Event Incidence Management solution (testing a computer log collection solution), SOAR testing (automating routine manual activities), exploring Industrial Control System and Supervisory Data Acquisition solution. We will add four new tools in FY 2022. In prior years, the tools budgets have been limited which hindered the ability to fully execute the Tools procurement and license renewals requirements. The increase will allow the PM to procure an increased number of tools to the cyber defenders, due to a rapid and dynamically changing threat, and the procurement of license renewals not covered in previous years. This will allow PM DCO to meet ARCYBER's requirements. This will also allow PM DCO to procure capabilities like High Speed Data Transport, Discovery (cloud), Single Node Solutions, Security Event Incidence Management solution, intel, continuous monitoring professional services, training, professional services for the Forge and Armory DevSecOps capabilities, support for the Tactical Server Infrastructure and

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
software support for ARCYBER. That software support includes the aforementioned, an operating system, command and control, network visualization, ISCADA, Hunt, clearing and remediation, program management, terrain analysis and packet capture.			
Title: Defensive Cyber Operations (DCO) - User Activity Monitoring (PEO EIS)	-	3.639	13.000
Description: DCO User Activity Monitoring is the primary capability within the Army's overall Insider Threat (InT) program. UAM is mainly a software-based, scalable solution that has an on-premise solution and a cloud solution. It 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 RDTE Plans: $3.639M FY 2021 funding supports development engineering, integration, and testing of multiple milestones broken into two phases. These milestones support the refinement of the on-premise solution as well as the engineering of the cloud solution. These solutions provide protection against Insider Threat through the deployment of capability in defense of our most critical networks. It also proactively identifies and mitigates internal risks associated with the theft or misuse of critical, mission essential data. It assists with the establishment of the Army's Insider Threat Protection Program that utilizes full-spectrum solutions to assess, deter, and evolve against the Insider Threat. This capability facilitates the ability to identify 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. It integrates the behavioral pattern analysis capability through the use of the Army's Big Data Platform (BDP). The Army will implement UAM for all Soldiers, Civilians, and Contractors with access to JWICS and SIPRNet. ***FY 2022 Plans:*** FY 2022 RDTE Plans: $11.590M FY 2022 funding supports development engineering, integration, and testing of the cloud based UAM Capability Suite to support ARCYBER and the CIO-G6 Special Access Program (SAP) Community. This entails continued behavioral pattern analysis, license renewals and maintenance, expanding production to tactical end point users, and transition from the on-premise solution to the cloud solution with the Army's Big Data Platform. FY 2022 focuses on the deployable UAM capability that will be configured to monitor, capture, and analyze data in a congested, complex, and highly contested cyberspace and electromagnetic environment. The capability at the tactical level will be tailored to send alerts to a higher level analysis cell (ex. Regional Cyber Center or Combatant Command Joint Cyber Center). FOC will be achieved in 4QTR FY 2022. FY 2022 OMA Plans: $1.410M			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2022 funding support (1) PB cloud hosting for JWICS. UAM Cloud capability will utilize machine learning behavior anomaly detection and data visualization to identify security threats in near real-time. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding transferred from RDTE PE 0605041A EV5. Funding increase will support procurement of annual licenses and license maintenance, development of UAM analytics, software engineering, integration, and testing of UAM Cloud Capability Suite. The increase in capabilities in FY 2022 are critical to reaching FOC by the end of FY 2022. To achieve FOC by 4QTR FY 2022, production requires deployment to tactical environments, the User Entity Behavioral Analysis (UEBA) tool to be integrated to function as an application on the BDP, integration of the collection tool database with the BDP, implementation of a bi-directional cross-domain solution, support deployment of UAM cloud capability to Army SAP Enterprise Portal, and completion of the UAM cloud capability to support Insider Threat and UAM analysts within ARCYBER.			
Title: Defensive Cyber Operations (DCO) - Forensics and Malware Analysis (PEO EIS) ***Description:*** DCO Forensics and Malware Analysis (F&MA) 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 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 OMA Plans: $1.087M FY 2021 funding supports software procurement, integration, and testing for Initial Operating Capability (IOC). The F&MA requirement deploys forensics capability within each theater of operation enabling the Regional Cyber Centers (RCCs) and Cyber Protection Teams (CPTs) to conduct live forensics on critical assets. F&MA provides the 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. The F&MA PoR procured 800,000 EnCase Investigator perpetual licenses to conduct live forensics along with requisite training and professional services for deployment activities. Maintenance for EnCase Investigator must be renewed annually. Ida Pro was purchased to allow the ARCYBER F&MA cell to conduct malware analysis and will be an annual renewal.	-	1.087	3.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
The IOC target date will move from 2Q FY 2021 to 3Q FY 2021. Proof of Concept activities currently underway (and requested by ARCYBER) will inform their decision for the deployment of EnCase Investigator to meet the Army?s F&MA mission. Upon receipt of an approved Authority to Operate (ATO) and deployment decision, the F&MA PoR will move forward with the purchase of the SAFE Servers required for EnCase Investigator deployment. Training on the EnCase Investigator capability has been provided (IOC requirement). IOC shall be considered attained when minimum, viable F&MA capabilities are met; the capability can be utilized by the ARCYBER F&MA Cell, Cyber Protection Brigade (CPB), and RCCs; personnel at ARCYBER F&MA Cell, and RCCs have access to the necessary amount of application licenses to collect and analyze images/artifacts from supported organizations' information systems; those within the ARCYBER F&MA Cell and RCCs are fully trained and judged to be capable of analyzing images, artifacts, malware and producing reports/evidence files leading to the prevention , detection and/or recovery across the Army network enterprise. FY 2021 funding also supports prototype activities for the development of a Threat Deception (TD) capability for the Army. Global defenders require the ability to conduct TD operations to detect and respond to advanced persistent threat (APT) within the defended network enclave. Our Cyber Defenders employ this capability to conduct defensive cyberspace operations (DCO) internal defensive measures (DCO-IDM) to detect and respond to adversary malicious presence and actions. ***FY 2022 Plans:*** FY 2022 OPA Plans: $1.900M FY 2022 funding supports procurement of new F&MA tools and production of the classified threat deception solution. (Potential production contract under the OTA) FY 2022 OMA Plans: $1.100M FY 2022 funding supports licenses renewals, maintenance, professional services and potential training activities as well as the delivery of a Sandbox Solution to further meet malware analysis requirements defined in the RDP. The malware analysis capability is a software-based application (Ida Pro) utilized by global and regional defenders to analyze malicious code in a sandbox-like, virtual environment (hardware). The malware sandbox capability will allow cyberspace defenders to collaborate in a member-only, protected environment; submit malware samples, check samples against popular open source tools and identify malware families using correlation and visualization tools. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding transferred from OPA PE 0128B63000. FY 2022 funding increase will support activities to attain IOC of the Threat Deception (TD) solution identified during prototype activities.			
Title: Defensive Cyber Operations (DCO) - Threat Emulation (PEO EIS)	-	1.813	4.000

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
Description: DCO Threat Emulation capability is a software based suite of tools used to gain access to evaluated networks 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 RDTE Plans: $1.813M FY 2021 funding supports development engineering, integration, and testing. It provides software based capability that will allow Cyber Protection Teams (CPTs) to assess the ability of systems to withstand an advance persistent threat actor attack by evaluating the people and processes. In FY 2021, the prototype Threat Emulation capability will be assessed (in a closed network) at three different operational locations (RCC-Pacific, RCC-CONUS, and Cyber Quest) to ensure that the capability meets the user's need and identify areas that can be improved in the production phase. Once assessments are completed in the latter part of FY 2021, the capability will be moved into the production phase. This capability will be produced to exist within a contemporary operational environment made up of a collective set of conditions (derived from a composite of actual worldwide conditions) that pose realistic challenges and opportunities for training, leader development, and capabilities development. ***FY 2022 Plans:*** FY 2022 RDTE Plans: $4.000M FY 2022 funding supports the production phase and an increase in engineering, integration and testing. During this time, the work in the production phase will ensure that the capability meets all Risk Management Framework (RMF) requirements needed for the capability to be used in an open network. In addition, training, fielding, and support will be provided to IOC designated units (fielding planned for 1QTR FY 2022). ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding transferred from RDTE PE 0605041A EV5. In FY 2022, there is an increase in needed funding due to the focus on the production phase activities. Specifically, the increased workload to ensure that the capability meets all RMF requirements needed for the capability to be used in an open network. Also, IOC is planned for 1QTR FY 2022 and this entails additional costs associated with training, travel, fielding, and any adjustments needed to the capability before it is fielded to Soldiers.			
Title: Defensive Cyber Operations (DCO) - Management Services (PEO EIS)	-	9.130	14.919
Description: Funding provides program management services and support from a mix of government matrix personnel and contractor management services for implementation, fielding, system engineering, logistics, program management and acquisition support.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2021 Plans: FY 2021 RDTE Plans: $1.720M FY 2021 OPA Plans: $7.410M FY 2021 funding provides continued program management services and support from a mix of government matrix personnel and contractor management services for implementation, fielding, system engineering, logistics, program management and acquisition support. ***FY 2022 Plans:*** FY 2022 RDTE Plans: $2.070M FY 2022 OPA Plans: $12.849M FY 2022 funding provides continued program management services and support from a mix of government matrix personnel and contractor management services for implementation, fielding, system engineering, logistics, program management and acquisition support. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding increase will provide program management services and support to multiple efforts in all phases of the acquisition process. This includes Cyber Analytics, DCO Mission Planning, Tools Suite, User Activity Monitoring, Forensics and Malware Analysis, and Threat Emulation capabilities. It includes program management costs that pays for a mix of government matrix personnel and contractor management services for development, implementation, fielding, system engineering, logistics, program management and acquisition support.			
Title: Defensive Cyber Operations (DCO) - DCO Development Environment (PEO EIS) ***Description:*** DCO Development Environment (DCODE) (formerly Forge) is a physical and virtual assets that provides continual integration, upgrade, assess, optimization and Soldier operational environment. It is designed to provide centralized lifecycle management and consists of the following capabilities: (1) Forge - physical or virtual asset that provides integration and assessment capabilities during the development and integration phases of operations (centrally managed patching and security); and (2) Development Network - provides the capability to remote into multiple networks (provides safe and secure infrastructure framework for Cyber Protection Teams (CPTs)). ***FY 2022 Plans:*** FY 2022 RDTE Plans: $4.779M	-	-	4.779

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
FY 2022 funding transferred from RDTE PE 0605041A EV5. The funding will continue assessment of new cyber technologies within controlled environment, assesses capabilities in integrated environment, provides virtual training access 24/7 worldwide, and assesses/pushes approved enhancement remotely. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2021 funding is reported under RDTE PE 0605041A EV5.			
Title: Defensive Cyber Operations (DCO) - Rapid Cyber Prototyping (ARCYBER)	-	0.465	2.501
Description: ARCYBER Rapid Cyber Prototyping provides software based capabilities that can quickly respond to emerging cyber threats and keep up with threat technology; while supporting Multi-Domain operations. ARCYBER identifies potential development and prototyping efforts via Cyber Needs Forms (CNFs) based on operational feedback, changes in the operational information environment and/or trends of adversarial activity; which drive CONOP and Tactics Techniques and Procedures (TTP) modifications. These are separate and distinct from DCO programmed efforts already funded or budgeted for by PM DCO and are used to rapidly address a network threat/vulnerability. ***FY 2021 Plans:*** FY 2021 OPA Plans: $.465M ARCYBER will use FY 2021 funds for Rapid Cyber Prototyping of a capability to observe and analyze Publicly Available Information (PAI) posted on a mission determined social media platforms at high capture rates required to support multi-domain operations (MDO) and joint all domain operations (JADO); and secondly, ARCYBER will conduct operational prototyping of emerging technology and expand on specific capabilities within existing technology in the DCO, Information Operation (IO), and/or Electronic Warfare (EW) domain. ARCYBER will utilize the Soldier Touch Points and Early User feedback/engagement to further mature the capability for the 915th and other organic ARCYBER elements pursuant to MDTF support and AR 10-87 responsibilities. ***FY 2022 Plans:*** FY 2022 RDTE Plans: $2.501M ARCYBER will continue to leverage Limited Acquisition Authority (LAA) for solutions that will enable solving more complicated problems that span Cyber, EW, and IO domains through rapid prototyping and capability assessments, which is outside of approved Requirements Definition Packages (RDPs) but within the scope of the FY 2018-2022 IT Box. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2022 funding increase will allow ARCYBER to rapidly get after threats with prototypes that fall outside of existing RPDs being developed by PM DCO. The ARCYBER Technical Warfare Center (TWC) Technology Innovation Center (ARCTIC) will add			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
additional authorities to enter into Cooperative Research and Development Agreements (CRADAs) and Educational Partnership Agreements (EPAs), and enable ARCYBER to prototype, and develop rapid cyber solutions.			
Accomplishments/Planned Programs Subtotals	-	56.706	118.811

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

The DCO Information System Initial Capabilities Document (IS ICD) was approved on 19 December 1017 by the Army Requirements Oversight Council (AROC). DCO programs are under an IT Box construct with five year term (FY 2018-2022) which aligns with current Requirements Definition Packages (RDPs). IT Box establishes funding thresholds, by appropriation, for a program over the capability's projected lifecycle of five (5) years. Current IT Box will expire in 4QTR FY 2022 and planned to be renewed in 1QTR FY 2022.

The Milestone Decision Authority (MDA), approved the Materiel Development Decision (MDD) on 13 April 2018, designating Tactical DCO Infrastructure (TDI) as an ACAT III program. The TDI program's RDP was approved on 8 November 2018 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. TDI is hosted on the Tactical Server Infrastructure (TSI) and will be fielded by the Command Post Computing Environment/TSI program in accordance with their fielding schedule. The TDI program had a Full Deployment Decision (FDD) of TDI's initial capability approved by the MDA on September 2019, which allowed the program to achieve IOC 1QTR FY 2020. TDI Full Deployment is currently planned for 4QTR FY2022 and is defined as, completion of development and testing of the last capability drop within the IT Box (reaching full functional values of the RDP), and transfer of the capability to the CPCE/TSI program to commence fielding. 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 18 May 2018; Mission Planning on 8 November 2018; User Activity Monitoring and Forensics and Malware Analysis on 18 March 2019; and Threat Emulation on 24 August 2020. The DCODE RDP approval is targeted for 4QFY2021. 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 FY 2018 National Defense Authorization Act (NDAA) Section 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 2022 Army			Date: May 2021
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 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO -Tactical DCO Infrastructure (TDI) (PEO C3T)	C/FFP	CACI : Aberdeen Proving Ground, (APG) MD	-	-		0.378		0.582	Mar 2022	-		0.582	Continuing	Continuing	-
DCO - Management Services (PEO EIS)	SS/TBD	Various : Various	-	-		9.130	Feb 2021	14.919	Feb 2022	-		14.919	Continuing	Continuing	-
		Subtotal	-	-		9.508		15.501		-		15.501	Continuing	Continuing	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical DCO Infrastructure (TDI) (PEO C3T)	C/CPFF	Parsons : Aberdeen Proving Ground, (APG) MD	-	-		3.468		4.176	Dec 2021	-		4.176	Continuing	Continuing	-
DCO - Cyber Analytics (PEO EIS)	C/FFP	Army Contracting Command - Rock Island (ACC-RI) : Rock Island, IL	-	-		16.187	Mar 2021	35.800	Mar 2022	-		35.800	Continuing	Continuing	-
DCO - Tools Suite (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		18.285	Mar 2021	26.267	Mar 2022	-		26.267	Continuing	Continuing	-
DCO - Mission Planning (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		1.100	Feb 2021	9.000	Feb 2022	-		9.000	Continuing	Continuing	-
DCO - User Activity Monitoring (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		3.639	Feb 2021	13.000	Feb 2022	-		13.000	Continuing	Continuing	-
DCO - Forensics and Malware (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		1.087	Mar 2021	3.000	Mar 2022	-		3.000	Continuing	Continuing	-
DCO - Threat Emulation (PEO EIS)	C/FFP	ACC-RI : Rock Island, IL	-	-		1.813	Feb 2021	4.000	Feb 2022	-		4.000	Continuing	Continuing	-
DCO - Rapid Cyber Prototyping (ARCYBER)	C/FFP	ACC-RI : Rock Island, IL	-	-		0.465	Apr 2021	2.501	Apr 2022	-		2.501	Continuing	Continuing	-
		Subtotal	-	-		46.044		97.744		-		97.744	Continuing	Continuing	N/A

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

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract

Remarks

TDI FY21 to FY22 funding increase will provide additional engineering to support completion/Full Deployment of the current IT Box (which plans to be renewed).

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical Development Infrastructure (TDI) (PEO C3T)	MIPR	DLA : Philadelphia, PA	-	-		0.115		0.213	Jun 2022	-		0.213	Continuing	Continuing	-
		Subtotal	-	-		0.115		0.213		-		0.213	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
DCO - Tactical Development Infrastructure (TDI) (PEO C3T)	C/FFP	CACI : Aberdeen Proving Ground, (APG) MD	-	-		1.039		0.574	Mar 2022	-		0.574	Continuing	Continuing	-
DCO - DCO Development Environment (PEO EIS)	MIPR	ATEC, SEC and TYAD : Various	-	-		-		4.779	Jan 2022	-		4.779	Continuing	Continuing	-
		Subtotal	-	-		1.039		5.353		-		5.353	Continuing	Continuing	N/A

Remarks

TDI FY21 to FY22 funding decrease due to a reduced amount of testing required. Further efficiency gained through consolidated PM Mission Command test events as a result of leveraging much of the same equipment and support personnel.

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	-		56.706		118.811		-		118.811	Continuing	Continuing	N/A

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

	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract

Remarks

FY22 TDI contract award dates reflect when contract option years plan to be exercised/when funding plans to be obligated.

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

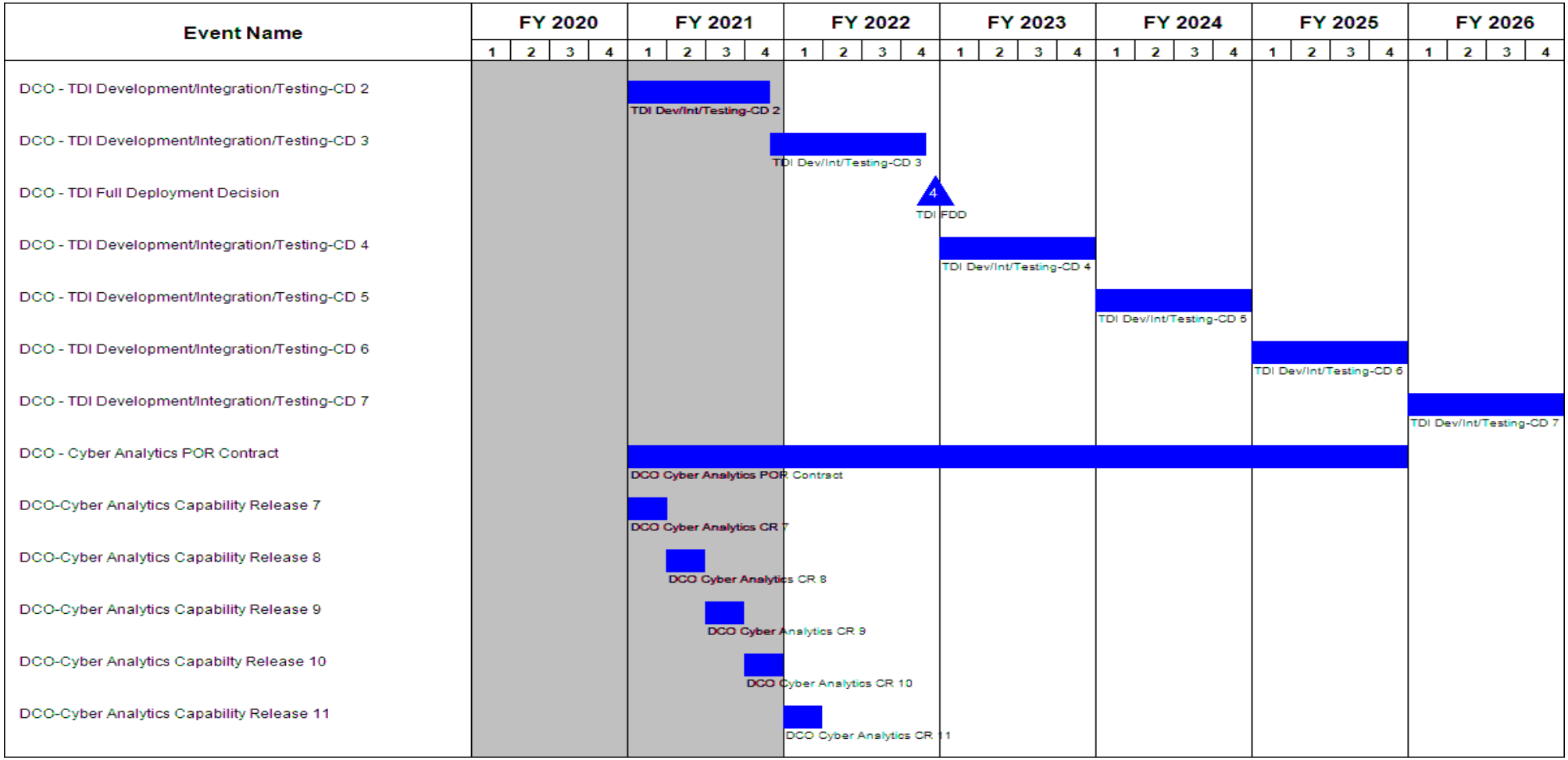

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

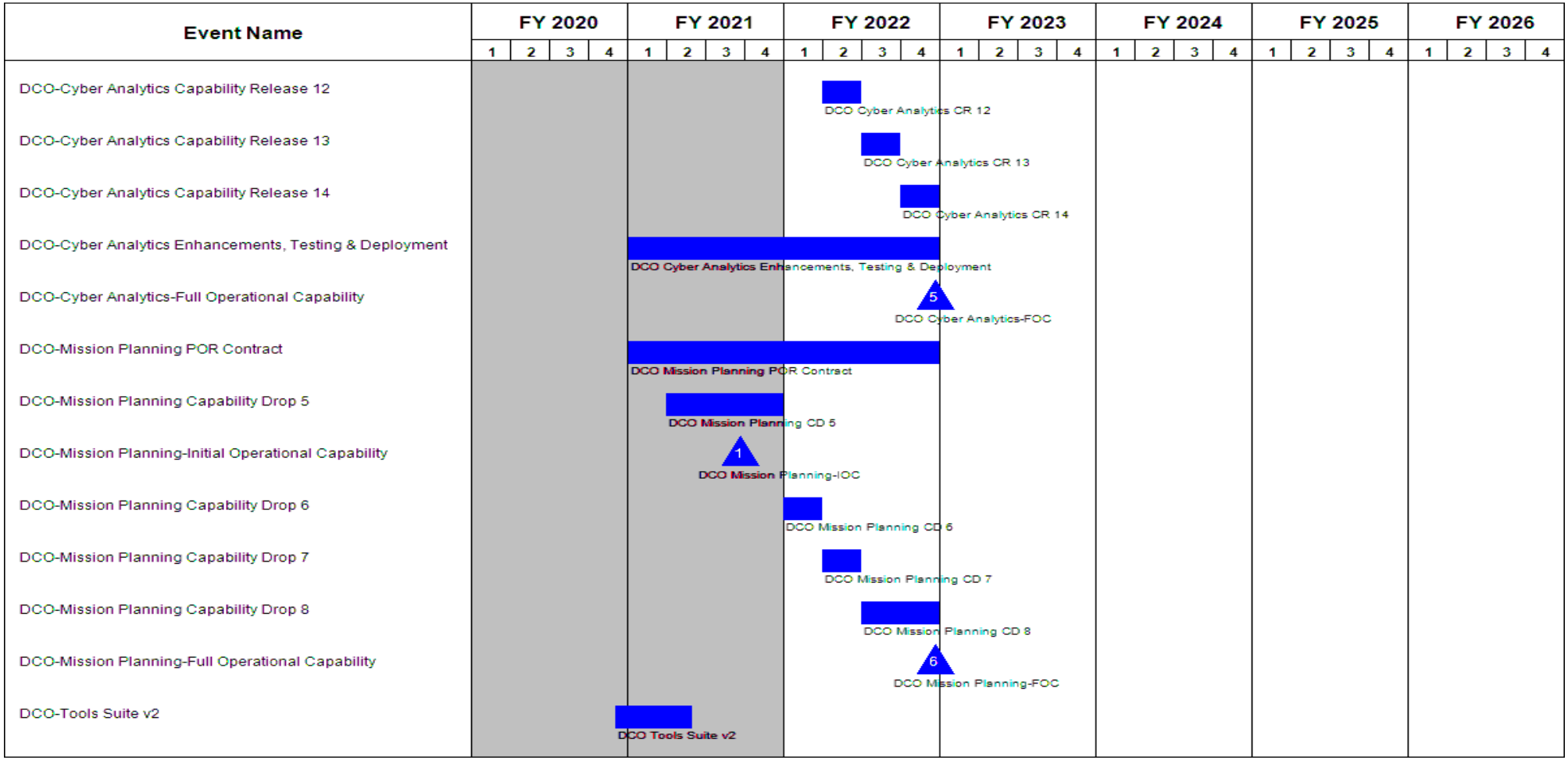

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

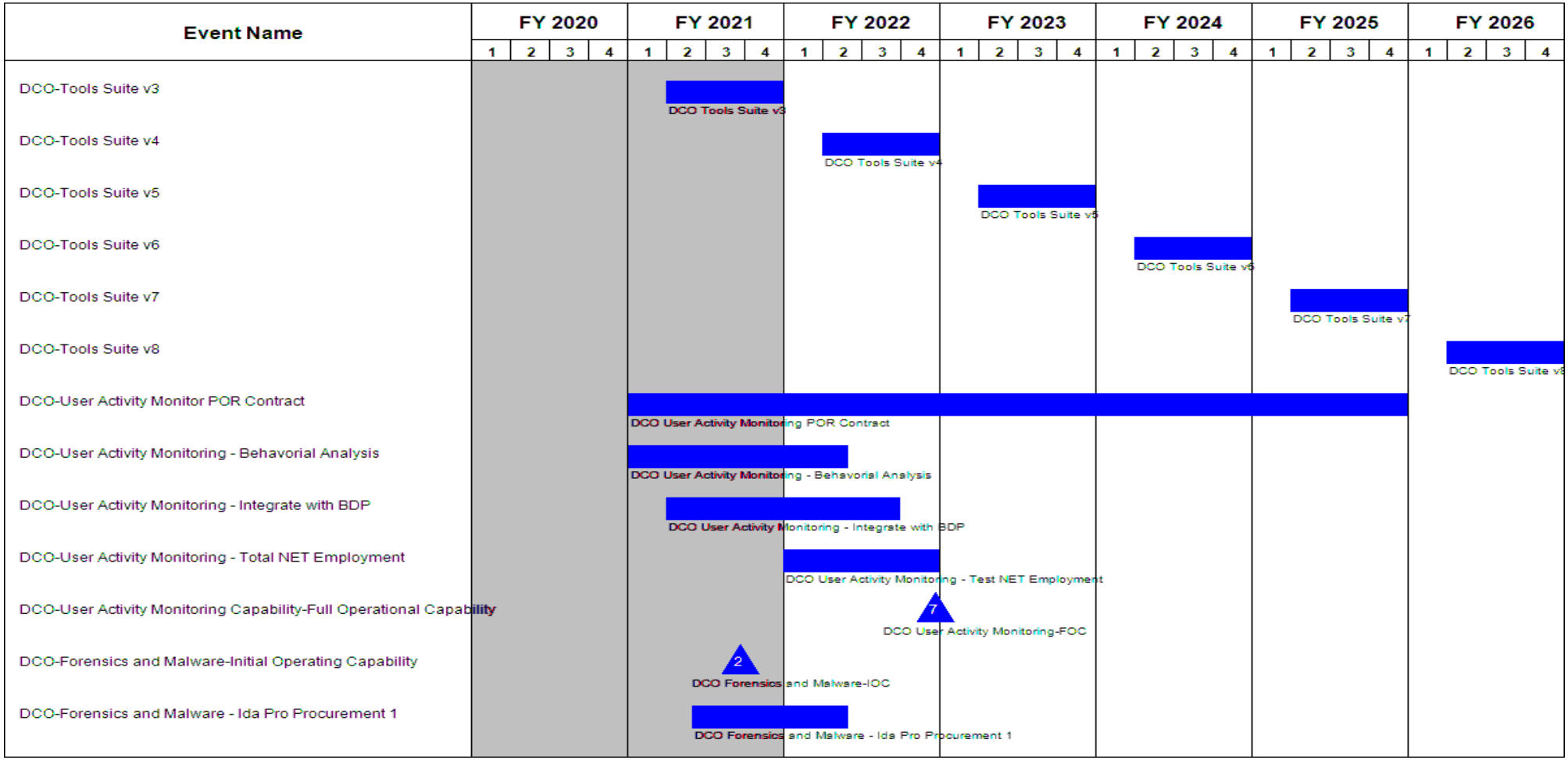

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

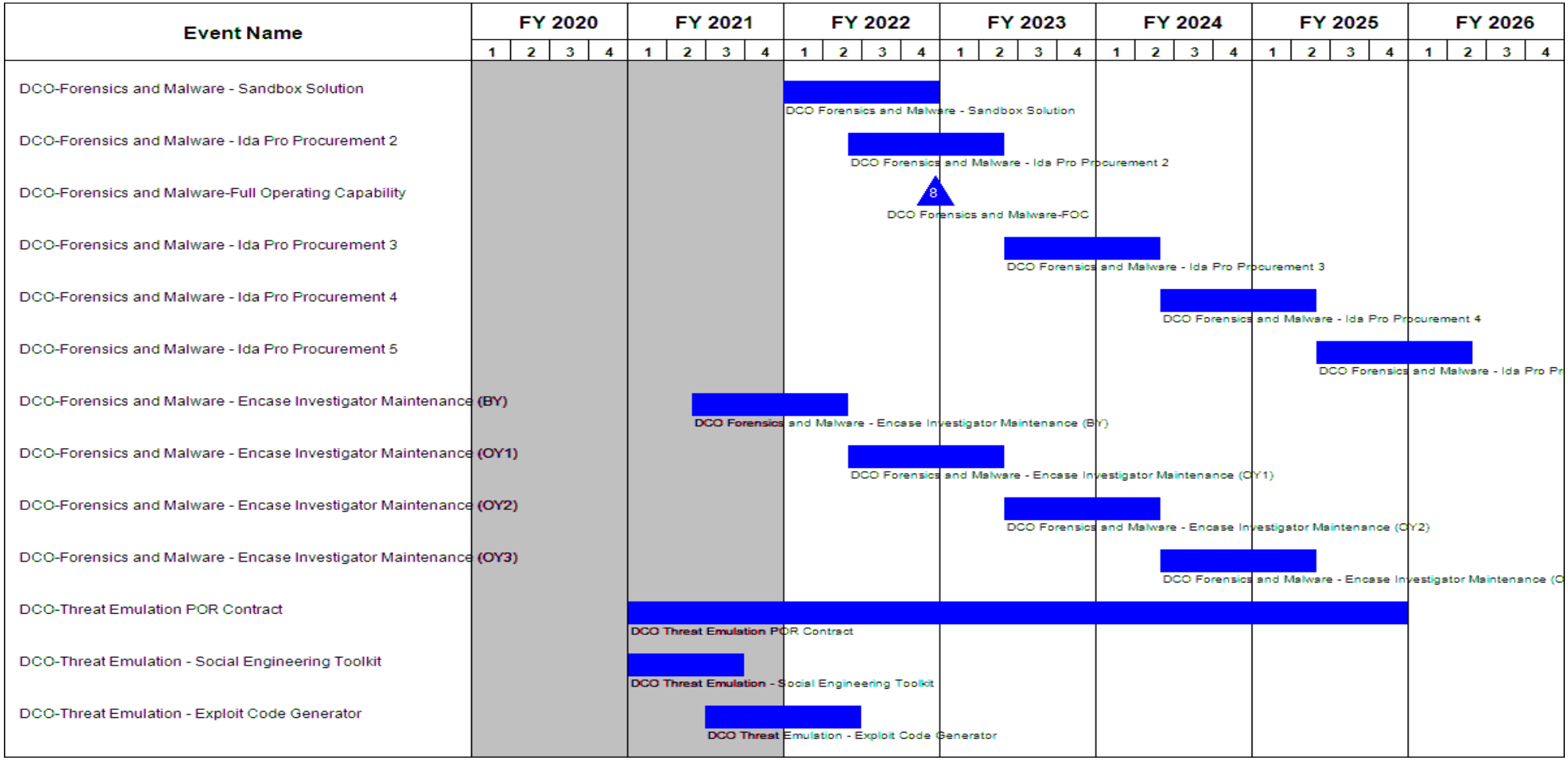

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

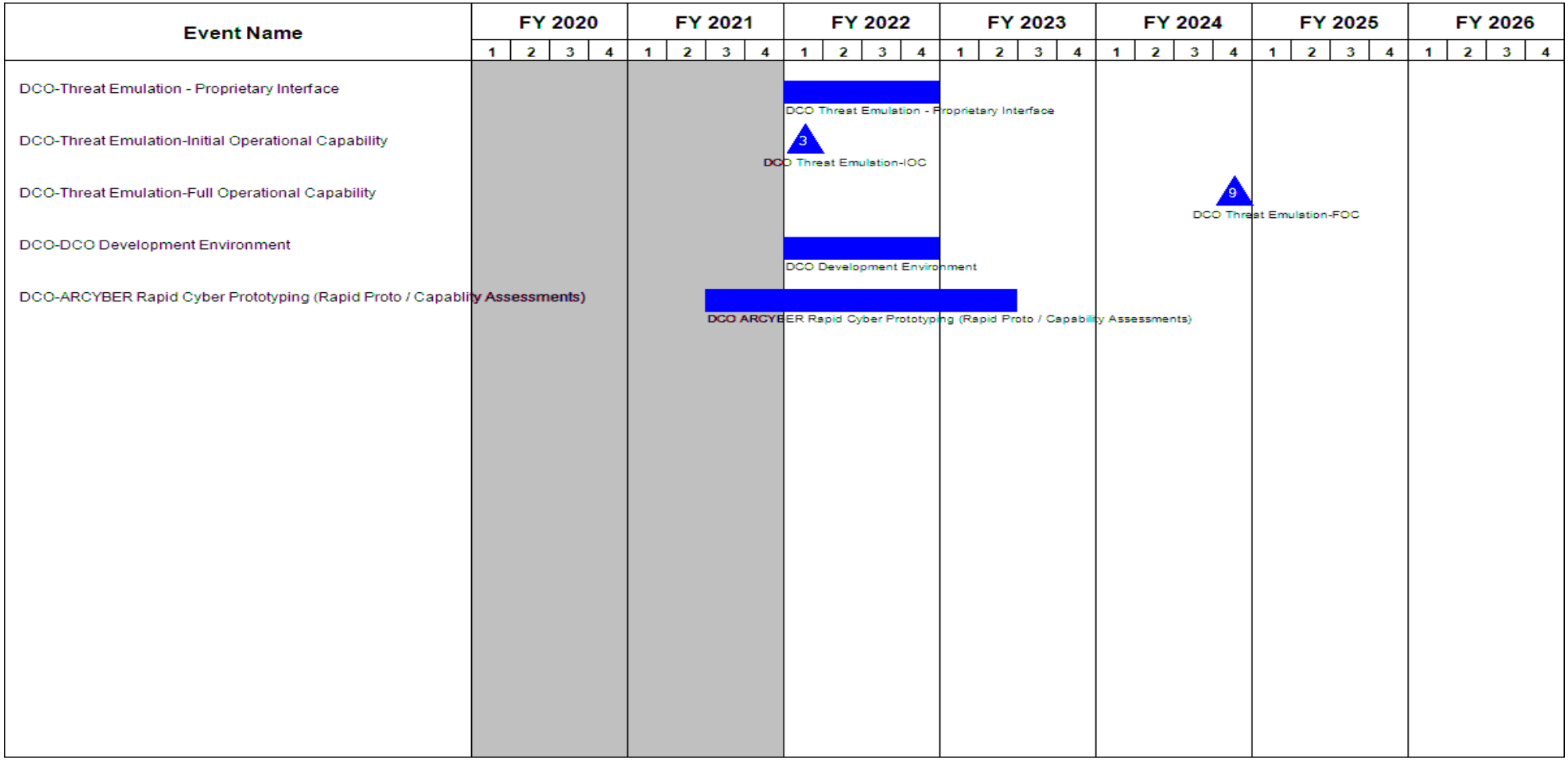

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 8	**R-1 Program Element (Number/Name)** PE 0608041A / *Defensive CYBER - Software Prototype Development*	**Project (Number/Name)** CD1 / *Defensive Cyber - Software Prototype Devel*

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 Full Deployment Decision	4	2022	4	2022
DCO - TDI Development/Integration/Testing-CD 4	1	2023	4	2023
DCO - TDI Development/Integration/Testing-CD 5	1	2024	4	2024
DCO - TDI Development/Integration/Testing-CD 6	1	2025	4	2025
DCO - TDI Development/Integration/Testing-CD 7	1	2026	4	2026
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 Enhancements, Testing & Deployment	1	2021	4	2022
DCO-Cyber Analytics-Full Operational Capability	4	2022	4	2022
DCO-Mission Planning POR Contract	1	2021	4	2022
DCO-Mission Planning Capability Drop 5	2	2021	4	2021
DCO-Mission Planning-Initial Operational Capability	3	2021	3	2021
DCO-Mission Planning Capability Drop 6	1	2022	1	2022

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
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-Mission Planning Capability Drop 7	2	2022	2	2022
DCO-Mission Planning Capability Drop 8	3	2022	4	2022
DCO-Mission Planning-Full Operational Capability	4	2022	4	2022
DCO-Tools Suite v2	4	2020	2	2021
DCO-Tools Suite v3	2	2021	4	2021
DCO-Tools Suite v4	2	2022	4	2022
DCO-Tools Suite v5	2	2023	4	2023
DCO-Tools Suite v6	2	2024	4	2024
DCO-Tools Suite v7	2	2025	4	2025
DCO-Tools Suite v8	2	2026	4	2026
DCO-User Activity Monitor POR Contract	1	2021	4	2025
DCO-User Activity Monitoring - Behavorial Analysis	1	2021	2	2022
DCO-User Activity Monitoring - Integrate with BDP	2	2021	3	2022
DCO-User Activity Monitoring - Total NET Employment	1	2022	4	2022
DCO-User Activity Monitoring Capability-Full Operational Capability	4	2022	4	2022
DCO-Forensics and Malware-Initial Operating Capability	3	2021	3	2021
DCO-Forensics and Malware - Ida Pro Procurement 1	2	2021	2	2022
DCO-Forensics and Malware - Sandbox Solution	1	2022	4	2022
DCO-Forensics and Malware - Ida Pro Procurement 2	2	2022	2	2023
DCO-Forensics and Malware-Full Operating Capability	4	2022	4	2022
DCO-Forensics and Malware - Ida Pro Procurement 3	2	2023	2	2024
DCO-Forensics and Malware - Ida Pro Procurement 4	2	2024	2	2025
DCO-Forensics and Malware - Ida Pro Procurement 5	2	2025	2	2026
DCO-Forensics and Malware - Encase Investigator Maintenance (BY)	2	2021	2	2022
DCO-Forensics and Malware - Encase Investigator Maintenance (OY1)	2	2022	2	2023

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
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-Forensics and Malware - Encase Investigator Maintenance (OY2)	2	2023	2	2024
DCO-Forensics and Malware - Encase Investigator Maintenance (OY3)	2	2024	2	2025
DCO-Threat Emulation POR Contract	1	2021	4	2025
DCO-Threat Emulation - Social Engineering Toolkit	1	2021	3	2021
DCO-Threat Emulation - Exploit Code Generator	3	2021	2	2022
DCO-Threat Emulation - Proprietary Interface	1	2022	4	2022
DCO-Threat Emulation-Initial Operational Capability	1	2022	1	2022
DCO-Threat Emulation-Full Operational Capability	4	2024	4	2024
DCO-DCO Development Environment	1	2022	4	2022
DCO-ARCYBER Rapid Cyber Prototyping (Rapid Proto / Capablity Assessments)	3	2021	2	2023

Note

TDI field decisions will occur after the completion of each TDI capability drop.

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).

Current DCO and TDI IT box ends in FY 2022. Army Capabilities Manager (ACM), formerly TRADOC Capability Manager (TCM)) is working to renew the IT Box construct for FY 2023-2027.