Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army											Date: March 2024	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 3: *Advanced Technology Development (ATD)*					R-1 Program Element (Number/Name) PE 0603457A *I C3I Cyber Advanced Development*							
COST ($ in Millions)	**Prior Years**	**FY 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
Total Program Element	-	41.354	28.847	19.616	-	19.616	21.377	24.598	34.201	33.607	0.000	203.600
6CY: *Autonomous Cyber Advanced Technology*	-	11.188	7.528	5.848	-	5.848	8.924	10.560	19.582	16.960	0.000	80.590
8CY: *Information Trust Advanced Technology*	-	20.028	11.187	4.188	-	4.188	3.006	4.910	5.864	6.186	0.000	55.369
9CY: *Network Access and Effects Advanced Technology*	-	8.170	10.132	9.580	-	9.580	9.447	9.128	8.755	10.461	0.000	65.673
CB4: *Offensive Cyber Operations (OCO) Mirror Adv Tech*	-	1.968	-	-	-	-	-	-	-	-	0.000	1.968

A. Mission Description and Budget Item Justification

This Program Element (PE) matures and demonstrates technologies for offensive and defensive cyber operations in tactical environments. Projects optimize devices, techniques, services, software and algorithms to enable cyber situational understanding and Cyber Electromagnetic Activities (CEMA). For offensive cyber, efforts demonstrate integrated electronic attack (EA) and CEMA hardware and software to execute force protection (FP), EA, electronic surveillance (ES), signals intelligence (SIGINT), electronic warfare (EW) and cyber missions in a dynamic, distributed and coordinated fashion. For defensive cyber, efforts demonstrate hardware and software to protect tactical wired and wireless networks against modern cyber attacks and focuses on configuration, operation, monitoring, data integrity, and defense in bandwidth constrained tactical environments while reducing the operator workload required to conduct these functions.

This PE directly supports the Network Army Modernization Priority.

The cited research is consistent with the Under Secretary of Defense for Research and Engineering priority focus areas and the Army Modernization Strategy.

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army					Date: March 2024
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 3: *Advanced Technology Development (ATD)*			R-1 Program Element (Number/Name) PE 0603457A *I C3I Cyber Advanced Development*		
B. Program Change Summary ($ in Millions)	**FY 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**
Previous President's Budget	41.354	28.847	19.204	-	19.204
Current President's Budget	41.354	28.847	19.616	-	19.616
Total Adjustments	0.000	0.000	0.412	-	0.412
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	0.412	-	0.412

Change Summary Explanation

The change in FY 2025 funding from the previous PB to the current PB reflects the net effect of a realignment from PE 0603457A / C3I Cyber Advanced Development to PE 0603463A (Network C3I Advanced Technology) for mid-to-long term efforts to develop and demonstrate new Signals Intelligence (SIGINT) methods and a realignment of funding to PE 0603457A / C3I Cyber Advanced Development from PE 0602213A / C3I Applied Cyber for efforts in support of the DoD Zero Trust Strategy.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
Appropriation/Budget Activity 2040 / 3	R-1 Program Element (Number/Name) PE 0603457A / *C3I Cyber Advanced Development*	Project (Number/Name) 6CY / *Autonomous Cyber Advanced Technology*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
6CY: *Autonomous Cyber Advanced Technology*	-	11.188	7.528	5.848	-	5.848	8.924	10.560	19.582	16.960	0.000	80.590
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project demonstrates defensive effects to adversarial use of artificial intelligence (AI) and machine learning (ML) to avoid detection and deceive our automated technologies driving the network decisions. This Project will provide defensive cyber operations (DCO) software capabilities for multi-domain operations and enable tactical network cyber defenders with machine learning (ML) and artificial intelligence (AI) capabilities.

Work in this Project complements Program Element (PE) 0602213A (C3I Applied Cyber) / Project CY6 (Autonomous Cyber Technology).

The cited work is consistent with the Under Secretary of Defense for Research and Engineering priority focus areas and the Army Modernization Strategy.

Work in this Project is performed by the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Autonomous Cyber	11.188	7.528	-
Description: This effort develops proof-of-concept sensors that can adapt to and autonomously react to adversary cyber-attack and develop a cyber response course of action decision aid for cyber defenders to validate suitability of actions and to speed response decisions. ***FY 2024 Plans:*** Will conduct final demonstration of hierarchical machine learning reference architecture supporting standardization of cyber capabilities that proactively react to and defend against advanced cyber threats and machine learning-enabled cyber-attacks to protect the network; conduct final assessment of the detection tools and autonomous decision-making system using adversarial attack simulation software tools to detect and self-mitigate any system vulnerabilities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding change reflects planned life cycle conclusion of this Science and Technology effort.			
Title: Predictive Intelligent Networking - Cyber	-	-	2.020
Description: This effort matures and validates network micro-segmentation methods based on tactical network constraints that employ artificial intelligence (AI) based advanced zero trust security features to autonomously identify, learn, predict, and react			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 3	**R-1 Program Element (Number/Name)** PE 0603457A / *C3I Cyber Advanced Development*	**Project (Number/Name)** 6CY / *Autonomous Cyber Advanced Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
to changes in network operating conditions, enables optimized resource quarantining and ensures end-to-end network resiliency against adversarial AI-driven electronic attacks (EA), electronic warfare (EW), and cyberattacks. ***FY 2025 Plans:*** Will mature various network micro-segmentation design patterns, based on the current Department of Defense (DoD) Zero Trust Reference Architecture, to determine lowest viable level for tactical networks. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort.			
Title: Network Obscuration and Deception ***Description:*** Mature and demonstrate software based cyber obscuration technologies; for use by Cyber Protection Teams (CPTs) and other cyber defenders in enterprise and tactical environments, utilizing planned Garrison and Tactical defensive Cyber Operations (DCO) Platforms; that imitate/mask networks, systems, hosts, users and files to distract/disrupt cyber attackers. ***FY 2025 Plans:*** Will mature and demonstrate first iteration of machine learning (ML) based moderate fidelity cyber obscuration capabilities positioned in advance of mission execution that can be remotely enabled as needed. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort.	-	-	1.539
Title: Tactical Hardening for Quantum ***Description:*** Enable faster migration from existing PKI algorithms to Post Quantum Cryptography (PQC) algorithms that are safe from compromise by quantum computing. Demonstrate advanced encryption algorithms to secure Army tactical networks against quantum computing threats. ***FY 2025 Plans:*** Will assess hybrid certificates with combinations of the conventional algorithms and the NIST selected Post Quantum Cryptography (PQC) algorithms; evaluate advancements in state-of-the-art technologies, standards, and solutions identify where conventional crypto is used, identify migration strategies and develop migration procedures to help implement PQC migration with the least disruption to system operation. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort.	-	-	2.289
Accomplishments/Planned Programs Subtotals	11.188	7.528	5.848

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 3	**R-1 Program Element (Number/Name)** PE 0603457A / *C3I Cyber Advanced Development*	**Project (Number/Name)** 6CY / *Autonomous Cyber Advanced Technology*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
Appropriation/Budget Activity 2040 / 3	R-1 Program Element (Number/Name) PE 0603457A / *C3I Cyber Advanced Development*	Project (Number/Name) 8CY / *Information Trust Advanced Technology*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
8CY: *Information Trust Advanced Technology*	-	20.028	11.187	4.188	-	4.188	3.006	4.910	5.864	6.186	0.000	55.369
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project demonstrates enhanced awareness of the "provenance"/ origin of data traversing the network from originator to consumer (e.g. sensor to shooter) in the presence of cyber-attacks, ensuring that the data can be trusted, has not been modified or manipulated, and has been authenticated for use in real-time decision making.

Work in this Project complements Program Element (PE) 06022213A (C3I Applied Cyber) / Project 2CY (Information Trust Technology).

The cited work is consistent with the Under Secretary of Defense for Research and Engineering priority focus areas and the Army Modernization Strategy.

Work in this Project is performed by the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Information Trust Advanced Technology	6.532	7.119	-
Description: This Project applies and demonstrates leading edge commercial technologies such as blockchain and machine learning to provide assurance that data has not been tampered with anywhere along the transmission chain from originator to consumer (e.g. sensor to shooter). This Project leverages automated algorithms to detect anomalies that may occur in the presence of cyber-attacks, such as an attempt to manipulate data traversing the network and alert decision makers. ***FY 2024 Plans:*** Will demonstrate a complimentary suite of software capabilities to ensure the integrity, authenticity and provenance of data traversing the tactical network; provide a machine learning based integrity service to ensure chain of custody, a blockchain-enabled provenance tracker software, enabling automatic modification detection, and a trust score architecture for real-time, quantitative, analytics-based trustworthiness of messages and other data in transit in the presence of cyber attacks. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding change reflects planned life cycle conclusion of this Science and Technology effort.			
Title: Agile Virtual Enclave	13.496	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 3	**R-1 Program Element (Number/Name)** PE 0603457A / *C3I Cyber Advanced Development*	**Project (Number/Name)** 8CY / *Information Trust Advanced Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Description: This effort matures and demonstrates a Multi-Level Security (MLS) Access Guard to reduce hardware infrastructure required for US Government owned systems and develop a Mission Partner Environment (MPE) transfer cross domain solution (CDS) to enable data sharing with coalition partners.			
Title: PKI-Modernization/Dynamic Access Control for Tactical (DAC-T) ***Description:*** This effort will mature and demonstrate cryptographic algorithms that address Program Manager (PM) Mission Command (MC) gap of native ability to support PKI digital signature and Online Certificate Status Protocol (OCSP) certificate validation for the Variable Message Format (VMF) standard MIL-STD-2045-47001D in Disconnected, Interrupted, and Low-bandwidth (DIL) Networks. Furthermore, the effort will also mature and demonstrate dynamic fine-grained access control that migrates the Army from a network-centric to data-centric access control in alignment with Advanced zero trust principles by enhancing, speeding up and automating account provisioning and access for people and non-Person entities (NPE) (e.g., sensors, devices, web services, etc.). This will significantly reduce the workload/ burden for the soldier and improve the networks security posture by enforcing least privilege & just-in-time network access. ***FY 2024 Plans:*** Will optimize PM MC cryptographic algorithms and Online Certificate Status Protocol (OCSP) certificate validation capability and conduct lab-based risk reduction to demonstrate and assess PKI Modernization impacts on Mounted Mission Command's (MMCs) ability to send digitally signed VMF messages; provide recommended courses of action to the current MIL-STD-2045-47001E. ***FY 2025 Plans:*** Will mature and demonstrate Crypto Library SW & MIL-STD-2045-47001 message parser; mature and demonstrate DAC-T Design & Technology data package and Application Programming Interface (API) for each ICAM service. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase is an economic adjustment.	-	4.068	4.188
Accomplishments/Planned Programs Subtotals	20.028	11.187	4.188

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 3	**R-1 Program Element (Number/Name)** PE 0603457A / *C3I Cyber Advanced Development*	**Project (Number/Name)** 8CY / *Information Trust Advanced Technology*

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
Appropriation/Budget Activity 2040 / 3	R-1 Program Element (Number/Name) PE 0603457A / *C3I Cyber Advanced Development*	Project (Number/Name) 9CY / *Network Access and Effects Advanced Technology*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
9CY: *Network Access and Effects Advanced Technology*	-	8.170	10.132	9.580	-	9.580	9.447	9.128	8.755	10.461	0.000	65.673
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project matures and demonstrates advanced mission management tools and workflows, to promote efficient selection and sequencing of effects to support the agile deployment and execution of Offensive Cyber Operations (OCO) / Radio Frequency (RF) Enabled capabilities in the face of ever-advancing and evolving cyber security standards and practices adopted by industry and our adversaries that impede our ability to maintain cyber freedom of maneuver in support of Multi-Domain Operations (MDO). This includes automated mission planning, staging methodologies, and tools to evaluate and compare various courses of action that are dynamically replicated within appropriate rapid response environment(s). This Project will enable both mission planners and operators to cognitively keep pace with the complexity of near-peer engagements within Multi-Domain Operations (MDO).

Work in this Project complements Program Element (PE) 0602213A (C3I Applied Cyber) / Project 3CY (Network Access and Effects Technology).

The cited work is consistent with the Under Secretary of Defense for Research and Engineering priority focus areas and the Army Modernization Strategy.

Work in this Project is performed by the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Offensive Cyber Enabling Mission Support ***Description:*** This effort matures and demonstrates advanced mission management tools and workflows, to promote efficient selection and sequencing of effects to support the agile deployment and execution of OCO / RF Enabled capabilities.	8.170	-	-
Title: Network Exploitation Research and Development (NERD) Advanced Technology ***Description:*** This effort matures computer assisted/automated development of Offensive Cyber Operations (OCO)/Radio Frequency (RF) enabled effects against emerging and validated targets of interest (TOI) in conjunction with exploration of non-traditional attack vectors. Matures automated mission planning and staging methodologies and tools to evaluate and compare various courses of actions that are dynamically replicated within appropriate rapid response environment to enable both mission planner and operators to cognitively keep pace with the complexity of near-peer engagements within Multi-Domain Operations (MDO). ***FY 2024 Plans:***	-	10.132	9.580

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 3	**R-1 Program Element (Number/Name)** PE 0603457A / *C3I Cyber Advanced Development*	**Project (Number/Name)** 9CY / *Network Access and Effects Advanced Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Will begin development of Non-Traditional Offensive Cyber Operations (OCO)/Radio Frequency (RF) enabled access and effects that account for and circumvent modern cyber security practices against expanded targets of interest; initiate development of tools to augment and automate vulnerability exploitation as well as access and effect capability development to reduce offensive cyber and RF enabled mission timelines. ***FY 2025 Plans:*** Will mature and demonstrate OCO/RF-enabled access and effects against targets of interest, enabling the commander to hold targets at risks in support of mission objectives; validate computer-assisted development to expedite access and effect, and reduce OCO/RF mission timelines; optimize concepts that reduce OCO/RF-enabled mission time to readiness through firing solution automation capabilities. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Decrease due to realignment in the amount of $0.834 million to PE 0603463A (Network C3I Advanced Technology) for mid-to-long term efforts to develop and demonstrate new Signals Intelligence (SIGINT) methods.			
Accomplishments/Planned Programs Subtotals	8.170	10.132	9.580

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
Appropriation/Budget Activity 2040 / 3	R-1 Program Element (Number/Name) PE 0603457A / *C3I Cyber Advanced Development*	Project (Number/Name) CB4 / *Offensive Cyber Operations (OCO) Mirror Adv Tech*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
CB4: *Offensive Cyber Operations (OCO) Mirror Adv Tech*	-	1.968	-	-	-	-	-	-	-	-	0.000	1.968
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project matures and demonstrates methods, tools and techniques to enable rapid instantiation of an operationally relevant cyberspace environment supporting critical Offensive Cyber Operations (OCO) mission functions to include but not limited to development, exercise, mission rehearsal and provide technical reach back to units during operations.

Work in this Project complements Program Element (PE) 0602213A (C3I Applied Cyber) / Project 5CY (Offensive Cyber Operations (OCO) Mirror Technology).

The cited work is consistent with the Under Secretary of Defense for Research and Engineering priority focus areas and the Army Modernization Strategy.

Work in this Project is performed by the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Offensive Cyber Operations Mirror	1.968	-	-
Description: This effort matures and demonstrates methods, tools, and techniques to enable rapid instantiation of an operationally relevant cyberspace environment supporting critical OCO mission functions to include but not limited to development, exercise, mission rehearsal and provide technical reach back to units during operations.			
Accomplishments/Planned Programs Subtotals	1.968	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A