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 2: *Applied Research*					R-1 Program Element (Number/Name) PE 0602213A *I C3I Applied Cyber*							
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	-	13.605	22.714	28.656	-	28.656	24.273	22.855	17.549	16.871	0.000	146.523
2CY: *Information Trust Technology*	-	0.858	3.054	7.838	-	7.838	2.505	2.167	-	-	0.000	16.422
3CY: *Network Access and Effects Technology*	-	7.798	10.588	12.550	-	12.550	11.848	12.257	12.390	12.514	0.000	79.945
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	1.022	-	-	-	-	-	-	-	-	0.000	1.022
CY1: *Information Assurance and Network Resiliency Tech*	-	3.927	-	-	-	-	-	-	-	-	0.000	3.927
CY6: *Autonomous Cyber Technology*	-	-	9.072	8.268	-	8.268	9.920	8.431	5.159	4.357	0.000	45.207

Note

2CY / Information Trust Technology (Tactical Zero Trust) - Funding is realigned from Program Element (PE) 0602213A (C3I Applied Cyber) / Project CY6 (Autonomous Cyber Technology), and PE 0603457A (C3I Cyber Advanced Development) / Project 6CY (Autonomous Cyber Advanced Technology).
CY6 / Autonomous Cyber Technology(Network Obscuration) - In Fiscal Year (FY) 2025, this Project has a skip year.

A. Mission Description and Budget Item Justification

This Program element (PE) investigates, designs, and develops cyber architectures, software, tools, and techniques to enable Cyber Electromagnetic Activities (CEMA) to counter adversary communications and harden the Army's tactical communications networks against cyber attacks. For offensive cyber effort against adversary communications, efforts investigate capabilities to identify and capture data traversing targeted networks for detection, identification, exploitation, direction finding, geolocation, and denial of service. Defensive cyber efforts in this PE focus on hardening the Army's tactical network by investigating and applying robust cyber security technologies and techniques to advance software, algorithms and protocols utilized within tactical networks, to protect against nation state level cyber-attacks and maintain Warfighter confidence in network information by hardening the blue force attack surface.

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

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 2: *Applied Research*		R-1 Program Element (Number/Name) PE 0602213A *I C3I Applied Cyber*			
B. Program Change Summary ($ in Millions)	**FY 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**
Previous President's Budget	13.605	22.714	32.949	-	32.949
Current President's Budget	13.605	22.714	28.656	-	28.656
Total Adjustments	0.000	0.000	-4.293	-	-4.293
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-4.293	-	-4.293

Change Summary Explanation

Funding decrease realigned for PE 06022146A Quantum Sensing.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army											Date: March 2024	
Appropriation/Budget Activity 2040 / 2					R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*				Project (Number/Name) 2CY / *Information Trust 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**
2CY: *Information Trust Technology*	-	0.858	3.054	7.838	-	7.838	2.505	2.167	-	-	0.000	16.422

Note

2CY / Information Trust Technology (Tactical Zero Trust) - Funding is realigned from Program Element (PE) 0602213A (C3I Applied Cyber) / Project CY6 (Autonomous Cyber Technology), and PE 0603457A (C3I Cyber Advanced Development) / Project 6CY (Autonomous Cyber Advanced Technology).

A. Mission Description and Budget Item Justification

This Project develops defensive cyber technology to ensure that data traversing the network remains verified and has not been modified through unauthorized means. Project enhances system access without affecting personnel authentication processes, enhances awareness of user actions and intent within the network, and maintains information provenance from originator to consumer. It will also integrate zero trust principles where access to resources is granted based on continuous risk assessments.

Work in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 8CY (Information Trust Advanced 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 Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: PKI-Modernization & Dynamic Access Control for Tactical (DAC-T) Technology	0.858	3.054	-
Description: This effort will investigate cryptographic algorithms that address Program Manager (PM) Mission Command 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, this effort will investigate methods to enhance, speed up and automate 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 validate OCSP stapling techniques and certificate validation methods that can be integrated with the PM MC variable message format (VMF) parser; design and develop the DAC-T Provisioning functions and conduct experiments on merging and synchronizing of ICAM data from data sources across the DOD, Army and tactical levels in accordance with the Army ICAM			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** 2CY / *Information Trust Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Requirements Definition Package (RDP), Army ICAM Strategy, Army ICAM Attribute Specification and DoD ICAM Reference Design. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding decrease reflects planned conclusion of this effort and transition to Program Element 0603457A (C3I Cyber Advanced Development) / Project 8CY (Information Trust Advanced Technology).			
Title: Tactical Zero Trust ***Description:*** Investigate concepts of Zero Trust that can be adapted to tactical network architectures. Extend concepts developed under current Dynamic Access Control - Tactical (DAC-T) to include non-person entities (NPE) (e.g., systems, applications, devices, robotic process automation (RPA) & services). Create an efficient data-in-use service to limit decryption and exfiltration of high value information. Include graceful degradation of capability for Person/NPE access based on Indicators of Compromise (IoC). Investigate open standard methods to create playbooks while assuring safe parallel execution of such playbooks. Effort will mature a capability that performs adversarial assessments on machine learning models to make them more robust to adversarial manipulation. ***FY 2025 Plans:*** Will investigate novel methods and techniques for uniquely identifying non-personnel entities (NPE's) (e.g., systems, applications, devices,?robotic process automation (RPA) & services) where Public Key Infrastructure (PKI) certificates are not feasible, (ie. Physical Unclonable Functions (PUF's), Fast Identity Online (FIDO2), etc.) and provide the ability to map them to the Master Device Record (MDR); investigate novel methods and techniques for providing protections of Data in Use; investigate advanced ways to provide graceful, degraded access of resources based on indicators of compromise; research and investigate novel adversarial machine learning methods and techniques. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort. Funding is realigned from Program Element (PE) 0602213A (C3I Applied Cyber) / Project CY6 (Autonomous Cyber Technology), and PE 0603457A (C3I Cyber Advanced Development) / Project 6CY (Autonomous Cyber Advanced Technology).	-	-	7.838
Accomplishments/Planned Programs Subtotals	0.858	3.054	7.838

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 / 2					R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*				Project (Number/Name) 3CY / *Network Access and Effects 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**
3CY: *Network Access and Effects Technology*	-	7.798	10.588	12.550	-	12.550	11.848	12.257	12.390	12.514	0.000	79.945

A. Mission Description and Budget Item Justification

This Project investigates the application of machine learning technologies to assist in capability development and mission execution processes with respect to Offensive Cyber Operations (OCO)/Radio Frequency (RF) Enabled capabilities.

Work in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 9CY (Network Access and Effects Advanced 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 Command, Control, Computer, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Applied OCO Techniques and Analytics ***Description:*** This effort investigates the application of machine learning technologies to assist in capability development and mission execution processes with respect to OCO/RF Enabled capabilities.	7.798	-	-
Title: Network Exploitation Research and Development (NERD) Technology ***Description:*** This effort investigates computer assisted/automated methodologies and tools to reduce the timelines associated with the exploitation of emerging and validated targets of interest, the development of courses of action, and the execution of offensive attack capabilities in the cyber and radio frequency domains at the pace of a near-peer engagement on a highly complex battlefield of ever evolving cyberspace threats. ***FY 2024 Plans:*** Will investigate and characterize vulnerabilities of targets of interest to determine the effectiveness of existing access and effect capabilities; investigate the use of artificial intelligence reasoning engines, informed by battlefield intelligence/situation awareness data, and the feasibility of their application to interpreting commander's intent and deriving offensive cyber and/or RF platform firing solutions. ***FY 2025 Plans:***	-	10.588	12.550

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** 3CY / *Network Access and Effects Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Will investigate non-traditional access and effect vectors against emerging targets of interest that account for and circumvent traditional computer security practices. Will investigate software component designs that expedite the characterization of vulnerabilities with an increased likelihood of holding targets of interest at risk. Will determine necessary data enrichment from Offensive Cyber and RF platforms to identify the ideal non-kinetic firing options for increased target effectiveness. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned research and characterization activities. In Fiscal Year (FY) 2025 funding is realigned from Program Element (PE) 0602213A (C3I Applied Cyber) / Project 5CY (Offensive Cyber Operations (OCO) Mirror Technology).			
Accomplishments/Planned Programs Subtotals	7.798	10.588	12.550

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 / 2	R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*	Project (Number/Name) 5CY / *Offensive Cyber Operations (OCO) Mirror 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
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	1.022	-	-	-	-	-	-	-	-	0.000	1.022

Note

In Fiscal Year (FY) 2023, this Project was completed.

A. Mission Description and Budget Item Justification

This Project investigates, designs, and develops emerging cyber techniques and cyber situational awareness technologies to enhance Army capabilities. This Project leverages behavioral Modeling and Simulation to mitigate risks and investigates cyber collection and mapping technologies to offer real time cyber situational awareness to enable interpretation of current threats and predict future enemy activities. This allows commanders to develop operational courses of action in time to act decisively.

Work in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project CB4 (Offensive Cyber Operations (OCO) Mirror Adv Tech).

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 Technology	1.022	-	-
Description: Designs and develops emerging internet technologies that enable OCO infrastructure maneuver within the neutral (gray) cyberspace environment; conduct experiments within a modeling and simulation environment (to include behavioral components) to enhance rapid offensive cyber developed capabilities, cyber mission rehearsal, and training.			
Accomplishments/Planned Programs Subtotals	1.022	-	-

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 / 2	R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*	Project (Number/Name) CY1 / *Information Assurance and Network Resiliency 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
CY1: *Information Assurance and Network Resiliency Tech*	-	3.927	-	-	-	-	-	-	-	-	0.000	3.927

Note

In Fiscal Year (FY) 2024 this Project is restructured to Program Element (PE) 0602213A (C3I Applied Cyber Technology) / Project CY6 (Autonomous Cyber).

A. Mission Description and Budget Item Justification

This Project investigates, designs, and develops techniques for detecting, disrupting, understanding and predicting complex adversarial activities and their impacts for developing agile, adaptive maneuvers in defense of information and networks (Agile Cyber Maneuver and Resilience).

Work in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 8CY (Information Trust Advanced 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 Assurance and Network Resiliency Technology	3.927	-	-
Description: This effort designs and characterizes software for the protection of information and networks in wireless tactical environments. The goal is to develop software algorithms that detect and defeat malicious activities of adversaries in bandwidth constrained tactical networks.			
Accomplishments/Planned Programs Subtotals	3.927	-	-

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 / 2	R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*	Project (Number/Name) CY6 / *Autonomous Cyber 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
CY6: *Autonomous Cyber Technology*	-	-	9.072	8.268	-	8.268	9.920	8.431	5.159	4.357	0.000	45.207

Note

CY6 / Autonomous Cyber Technology(Network Obscuration) - In Fiscal Year (FY) 2025, this Project has a skip year.

A. Mission Description and Budget Item Justification

This Project investigates and applies robust cyber security techniques and applications to advanced communications and networking devices, software, algorithms and protocols utilized within wireless tactical networks to protect against nation state level cyber effects and maintain Warfighter confidence in network information, resources, identities and mission partners by hardening the blue force attack surface.

Work in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 6CY (Autonomous Cyber Advanced 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 Army Research Laboratory (ARL) and Command, Control, Computer, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Predictive Intelligent Networking (PIN)	-	1.739	3.833
Description: Investigate and develop various design patterns of Network Micro-segmentation given constraint of tactical network, conduct various experiments to determine the lowest viable level of Micro-segmentation for the tactical network, as there are different levels of fidelity of Micro-segmentation, and provide an implementation in support of advanced zero trust concepts. This project researches methods to enable the tactical network to autonomously identify, learn, predict, and react to changes in network operating conditions and network threats to ensure end-to-end network resiliency against adversarial AI-driven electronic attacks (EA), electronic warfare (EW), and cyberattacks.			
FY 2024 Plans: Will investigate hardware/software modules that are compatible with the current Mounted Mission Command Software (MMC-S) program of record, that can process collected spectrum data from multiple receivers and feed the predictive decision software with spectrum-aware information software			
FY 2025 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** CY6 / *Autonomous Cyber Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Will conduct experiments with various network micro-segmentation solutions, based on the current Department of Defense (DOD) Zero Trust Reference Architecture, to define logical network enclaves at the lowest levels that support the visibility and dynamic adaptations necessary to support security and trust while continuing to provide optimum network traffic flow and services at the tactical level. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase reflects planned experiment activities to determine lowest viable level for tactical networks.			
Title: Network Obscuration ***Description:*** Develops the capability to obscure cyberspace operations to delay/deter adversaries that attack and exploit blue cyberspace in enterprise or tactical networks. This project creates cyber obscuration technologies that imitate networks, systems, hosts, users and files that evolve as the network and missions change to distract/disrupt cyber attackers, mitigate or delay their attacks, increasing network resiliency and supporting operations in highly contested, DIL and cyberspace environments. ***FY 2024 Plans:*** Will leverage industry and National Security Agency's (NSA) Camouflage (CAMO) project, begin to investigate the use of machine learning to build obscuration techniques and modeling concepts for pre-placed, remotely administered network obscurations at the systems, applications, users, and data levels. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** In Fiscal Year (FY) 2025, this Project has a skip year.	-	2.959	-
Title: Proactive Cyber Defense ***Description:*** This effort designs and characterizes software for the protection of information and networks in wireless tactical environments. The goal is to develop software algorithms that detect and defeat malicious activities of adversaries in bandwidth and highly resource constrained tactical networks and maintain agile, adaptive cyber maneuver. This research provides automated active defense (e.g., machine learning, anomaly detection, and decision aids) and adversarial resilient techniques to maintain cyber superiority (e.g., improved attack detection, advanced network traffic analysis, and predictive decision aids) against a large attack surface at the edge. ***FY 2024 Plans:*** Will develop algorithms and methodologies for machine learning enabled network analysis tools; experiment with feature extraction, selection, and generation in testing phase of machine learning models for deep packet inspection; investigate network modality based Adversarial Machine Learning (AML) poisoning threats and defenses; develop techniques to improve the Intrusion Detection Systems (IDS) model performance through adversarial retraining; investigate the use of cyber agility and misrepresentation algorithms and methodologies as well as additional evasion defensive algorithms against Adversarial Machine	-	4.374	4.435

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** CY6 / *Autonomous Cyber Technology*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Learning (AML) in order to make tactical and enterprise systems resistant to attacks on their cyber defenses that rely on machine learning. ***FY 2025 Plans:*** Will investigate semi-supervised and self-supervised learning techniques for network intrusion detection that are resilient to adversarial attacks, do not require large amounts of labeled training data, and operate on resource constrained devices; investigate the use of cyber agility and misrepresentation algorithms and methodologies; investigate additional evasion defensive algorithms to make tactical and enterprise systems resistant to attacks on machine learning, which is heavily used by cyber defenses; develop machine learning based algorithms and methodologies to mitigate adversarial poisoning attempts on critical systems; develop high interaction honeynets/pots to misrepresent current networks and systems in tactical environments. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase is an economic adjustment.			
Accomplishments/Planned Programs Subtotals	-	9.072	8.268

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A