Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army											Date: March 2023	
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**Cost To Complete**	**Total Cost**
Total Program Element	-	12.119	13.605	22.714	-	22.714	32.949	25.591	22.414	16.672	0.000	146.064
2CY: *Information Trust Technology*	-	0.601	0.858	3.054	-	3.054	-	-	-	-	0.000	4.513
3CY: *Network Access and Effects Technology*	-	6.479	7.798	10.588	-	10.588	12.525	12.225	12.233	12.366	0.000	74.214
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	0.987	1.022	-	-	-	-	-	-	-	0.000	2.009
CY1: *Information Assurance and Network Resiliency Tech*	-	3.397	3.927	-	-	-	-	-	-	-	0.000	7.324
CY6: *Autonomous Cyber Technology*	-	0.655	-	9.072	-	9.072	20.424	13.366	10.181	4.306	0.000	58.004

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 2024 Army					Date: March 2023
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**
Previous President's Budget	12.119	13.605	25.231	-	25.231
Current President's Budget	12.119	13.605	22.714	-	22.714
Total Adjustments	0.000	0.000	-2.517	-	-2.517
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-2.517	-	-2.517

Change Summary Explanation

Decreased funding to support higher Army priorities.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
2CY: *Information Trust Technology*	-	0.601	0.858	3.054	-	3.054	-	-	-	-	0.000	4.513

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.

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 United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Information Trust Technology ***Description:*** This effort develops defensive cyber technology to ensure that data traversing the network remains verified and has not been modified through unauthorized means.	0.601	-	-
Title: PKI-Modernization & Dynamic Access Control for Tactical (DAC-T) Technology ***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 2023 Plans:*** Investigate modern PKI algorithms as well as OCSP stapling; investigate different courses of action for changes to the current MIL-STD-2045-47001E; update cryptographic libraries and software stack to support modern cryptographic algorithms and capabilities as well as OCSP Stapling; establish an Identity Credential & Access Management (ICAM) test infrastructure to test/ Integrate merging and synchronizing of ICAM data from data sources across the Department of Defense (DOD), Army and tactical levels in accordance with the Army ICAM Strategy, Army ICAM Attribute Specification and DoD ICAM Reference Design. ***FY 2024 Plans:***	-	0.858	3.054

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 Requirements Definition Package (RDP), Army ICAM Strategy, Army ICAM Attribute Specification and DoD ICAM Reference Design. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding increase enables the development of the DAC-T account provisioning capability and mature the cryptographic libraries.			
Accomplishments/Planned Programs Subtotals	0.601	0.858	3.054

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
3CY: *Network Access and Effects Technology*	-	6.479	7.798	10.588	-	10.588	12.525	12.225	12.233	12.366	0.000	74.214

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 the United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Applied OCO Techniques and Analytics	6.479	7.798	-
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. ***FY 2023 Plans:*** Complete technology readiness level (TRL) 4 OCO/RF enabled effects for an identified target of interest. Continue development of machine assisted technique development based on existing and known system vulnerabilities. Conduct experiments and assess the machine assisted techniques against targets of interest. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding decrease reflects planned conclusion of this effort and transitions to Project Element (PE) 0603457 (C3I Cyber Advanced Development) / Project 9CY (Network Access and Effects Advanced Technology).			
Title: Network Exploitation Research and Development (NERD) Technology	-	-	10.588
Description: This effort will investigate 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 2023 to FY 2024 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort.			
Accomplishments/Planned Programs Subtotals	6.479	7.798	10.588

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	0.987	1.022	-	-	-	-	-	-	-	0.000	2.009

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 United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Offensive Cyber Operations Mirror Technology	0.987	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. ***FY 2023 Plans:*** Develop and mature second increment of the Discrete Event Simulator user interface. Conduct assisted cyber maneuver development to assist in successful execution of cyber missions. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding reflects planned conclusion of this project.			
Accomplishments/Planned Programs Subtotals	0.987	1.022	-

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
CY1: *Information Assurance and Network Resiliency Tech*	-	3.397	3.927	-	-	-	-	-	-	-	0.000	7.324

Note

In Fiscal Year (FY) 2024 this Project is realigned to Program Element (PE) 0602213A (C3I Applied Cyber Technology) / Project CY6 (Autonomous Cyber) to streamline the cyber portfolio by consolidating cyber applied research under one Project.

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 United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Information Assurance and Network Resiliency Technology	3.397	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. ***FY 2023 Plans:*** Develop algorithms and methodologies for machine learning enabled network analysis tools (e.g. deep packet inspection); experiment with feature extraction, selection, and generation in testing phase of machine learning models for deep packet inspection; investigate network modality based AML poisoning threats and defenses; develop techniques to improve the Intrusion Detection Systems (IDS) model performance through adversarial retraining. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding administratively realigned to PE 0602213A Project CY6 Autonomous Cyber Technology to streamline the cyber portfolio by consolidating cyber applied research under one Project.			
Accomplishments/Planned Programs Subtotals	3.397	3.927	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
CY6: *Autonomous Cyber Technology*	-	0.655	-	9.072	-	9.072	20.424	13.366	10.181	4.306	0.000	58.004

Note

In Fiscal Year (FY) 2024 effort from PE 0602213A (Autonomous Cyber Technology) / Project CY1 (Information Assurance and Network Resiliency Tech) was administratively realigned to Project CY6 to streamline the cyber portfolio by consolidating cyber applied research under one Project.

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 United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Autonomous Cyber Technology ***Description:*** This effort develops defensive cyber technology to secure the automated network decisions (e.g., Primary, Alternate, Contingency, and Emergency (PACE)) and defend against adaptive, autonomous cyber-attacks at machine speed.	0.655	-	-
Title: Predictive Intelligent Networking (PIN) ***Description:*** Enables the tactical network with algorithms that autonomously identify, learn, predict and react seamlessly to changes in the network. Uses machine learning enabled drivers to ensure end-to-end network communications resiliency against adversarial AI-enabled Electronic Attacks (EA), Electronic Support (ES), 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 2023 to FY 2024 Increase/Decrease Statement:***	-	-	1.739

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
Funding increase reflects planned initiation of this effort			
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 to distract/disrupt cyber attackers to mitigate or delay their attacks thereby increasing network resiliency ***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 2023 to FY 2024 Increase/Decrease Statement:*** Funding increase reflects planned initiation of this effort	-	-	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 constrained tactical networks and maintain agile, adaptive cyber maneuver. ***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 Learning (AML) in order to make tactical and enterprise systems resistant to attacks on their cyber defenses that rely on machine learning. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** In FY 2024, funding administratively realigned from PE 0602213A (C3I Applied Cyber Technology) / Project CY1 (Information Assurance and Network Resiliency Tech) to streamline the cyber portfolio by consolidating cyber applied research under one Project.	-	-	4.374
Accomplishments/Planned Programs Subtotals	0.655	-	9.072

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** CY6 / *Autonomous Cyber Technology*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A