Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army											Date: April 2022	
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 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**Cost To Complete**	**Total Cost**
Total Program Element	-	18.816	12.119	13.605	-	13.605	25.231	36.203	28.263	26.690	0.000	160.927
2CY: *Information Trust Technology*	-	1.220	0.601	0.858	-	0.858	3.041	-	-	-	0.000	5.720
3CY: *Network Access and Effects Technology*	-	4.191	6.479	7.798	-	7.798	10.541	12.455	12.146	12.143	0.000	65.753
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	0.999	0.987	1.022	-	1.022	-	-	-	-	0.000	3.008
CI6: *Network Obscuration and Deception Tech**	-	-	-	-	-	-	3.078	3.951	1.774	-	0.000	8.803
CY1: *Information Assurance and Network Resiliency Tech*	-	3.488	3.397	3.927	-	3.927	4.215	4.254	10.377	12.993	0.000	42.651
CY6: *Autonomous Cyber Technology*	-	6.133	0.655	-	-	-	4.356	15.543	3.966	1.554	0.000	32.207
CY8: *Cyber Security App Research and Exper Partner Tech*	-	2.785	-	-	-	-	-	-	-	-	0.000	2.785

*This project's R-2a exhibit has been suppressed due to funding not beginning until after FY 2023

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 2023 Army					Date: April 2022
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 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**
Previous President's Budget	18.816	12.123	0.000	-	0.000
Current President's Budget	18.816	12.119	13.605	-	13.605
Total Adjustments	0.000	-0.004	13.605	-	13.605
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	13.605	-	13.605
• FFRDC Transfer	-	-0.004	-	-	-

Change Summary Explanation

Fiscal Year 2023 (FY23) funding increase reflects the fact that the FY22 President's Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
2CY: *Information Trust Technology*	-	1.220	0.601	0.858	-	0.858	3.041	-	-	-	0.000	5.720

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.

Research in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 8CY (Information Trust Advanced Technology).

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

Research in this Project is performed by the United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Information Trust Technology	1.220	0.601	-
Description: This effort develops defensive cyber technology to ensure that data traversing the network remains verified and has not been modified through unauthorized means. ***FY 2022 Plans:*** Will mature and validate the trust score architecture that provides real time analytics of the data through distributed processing and minimization of network traffic. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Effort transitions to follow on work in PE 0603457A (C3I Cyber Advanced Development) / Project 8CY (Information Trust Advanced Technology)			
Title: PKI-Modernization & Dynamic Access Control for Tactical (DAC-T) Technology	-	-	0.858
Description: This effort is focused on modernizing the Army's Public Key Infrastructure (PKI). Cryptographic algorithms and addresses the 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. The Dynamic Access Control for Tactical (DAC-T) LOE enhances, speeds up and automates 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
FY 2023 Plans: Will investigate modern PKI algorithms as well as OCSP stapling; will investigate different courses of action for changes to the current MIL-STD-2045-47001E; will update cryptographic libraries and software stack to support modern cryptographic algorithms and capabilities as well as OCSP Stapling; will 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 2022 to FY 2023 Increase/Decrease Statement:*** New Effort in FY23			
Accomplishments/Planned Programs Subtotals	1.220	0.601	0.858

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
3CY: *Network Access and Effects Technology*	-	4.191	6.479	7.798	-	7.798	10.541	12.455	12.146	12.143	0.000	65.753

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.

Research in this Project complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) / Project 9CY (Network Access and Effects Advanced Technology).

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

Research in this Project is performed by the United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Applied OCO Techniques and Analytics	3.945	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 2022 Plans:*** Will conduct experiments of OCO/RF Enabled access and effects vectors against emerging AC4I targets of interest. Shall investigate software approaches to support vulnerability discovery against emerging targets of interest and conduct experiments to determine development time reduction. Will conduct experiments with decision aids leveraging machine learning to reduce cognitive burden on OCO/RF operators. ***FY 2023 Plans:*** Will complete technology readiness level (TRL) 4 OCO/RF enabled effects for an identified target of interest. Will continue development of machine assisted technique development based on existing and known system vulnerabilities. Will conduct experiments and assess the machine assisted techniques against targets of interest. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Funding increase reflects planned lifecycle of the program to conduct experiments to determine development time reduction of vulnerability discovery.			
Title: Command, Control and Communications Attack	0.246	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
Description: This effort investigates RF Enabled access and effects against adversary Command, Control, Communication, Computers, and Intelligence (AC4I) systems executed from agile OCO/RF Enabled firing platforms.			
Accomplishments/Planned Programs Subtotals	4.191	6.479	7.798

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
5CY: *Offensive Cyber Operations (OCO) Mirror Technology*	-	0.999	0.987	1.022	-	1.022	-	-	-	-	0.000	3.008

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.

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

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

Research in this Project is performed by the United States Army Futures Command (AFC).

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Offensive Cyber Operations Mirror Technology	0.999	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 2022 Plans:*** Will determine methodologies for assisted OCO maneuver and conduct experiments to enable fidelity driven Development Security Operations (DevSecOps) leveraging foundational modeling and simulation environments ***FY 2023 Plans:*** Will 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 2022 to FY 2023 Increase/Decrease Statement:*** Funding reflects planned lifecycle of project.			
Accomplishments/Planned Programs Subtotals	0.999	0.987	1.022

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
CY1: *Information Assurance and Network Resiliency Tech*	-	3.488	3.397	3.927	-	3.927	4.215	4.254	10.377	12.993	0.000	42.651

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).

This research complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) /Project 8CY (Information Trust Advanced Technology).

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

Research in this Project is performed by the United States Army Futures Command.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Information Assurance and Network Resiliency Technology	3.488	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 2022 Plans:*** Will develop, characterize, and conduct experiments on networking methods for unconventional communications modalities; design and develop adaptive networking protocols for the simultaneous operation of multiple communications modalities; implement and conduct experiments on multilayer network control algorithms for mission-centric network operation in complex environments including jamming; develop example of adversarial machine learning (AML) methods within a laboratory environment against existing cyber security classifiers, enhance network intelligence gathering, machine learning applications, and decoding tool capabilities; increase network forensics capabilities to adapt to more complex networks and protocols, investigating methods which may utilize Machine Learning and autonomous analysis; increase network situational awareness, enable sophisticated analysis and reverse engineering of current and emerging network protocols, and apply and assess foundational network security research algorithms. ***FY 2023 Plans:*** Will 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			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
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 2022 to FY 2023 Increase/Decrease Statement:*** Funding increase reflects planned lifecycle of this effort.			
Accomplishments/Planned Programs Subtotals	3.488	3.397	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 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
CY6: *Autonomous Cyber Technology*	-	6.133	0.655	-	-	-	4.356	15.543	3.966	1.554	0.000	32.207

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.

This research complements Program Element (PE) 0603457A (C3I Cyber Advanced Development) Project 6CY (Autonomous Cyber Advanced Technology).

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

Research in this Project is performed by the United States Army Futures Command (AFC).

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Autonomous Cyber Technology	6.133	0.655	-
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. ***FY 2022 Plans:*** Will mature and demonstrate proof-of-concept generative network algorithms and neural network software to simulate adversarial attacks on artificial intelligence / machine learning (AI/ML) algorithms that can be utilized to ensure trustworthiness of autonomous network configuration decisions and mitigate any vulnerable decisions. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Effort transitions to follow on work in PE 0603457A (C3I Cyber Advanced Development) / Project 6CY (Autonomous Cyber Advanced Technology).			
Accomplishments/Planned Programs Subtotals	6.133	0.655	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
Appropriation/Budget Activity 2040 / 2	**R-1 Program Element (Number/Name)** PE 0602213A / *C3I Applied Cyber*	**Project (Number/Name)** CY6 / *Autonomous Cyber Technology*

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
Appropriation/Budget Activity 2040 / 2	R-1 Program Element (Number/Name) PE 0602213A / *C3I Applied Cyber*	Project (Number/Name) CY8 / *Cyber Security App Research and Exper Partner Tech*	

COST ($ in Millions)	Prior Years	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
CY8: *Cyber Security App Research and Exper Partner Tech*	-	2.785	-	-	-	-	-	-	-	-	0.000	2.785

A. Mission Description and Budget Item Justification

This Project investigates cyber electromagnetic activities (CEMA), cyber security devices, software and techniques to harden wireless communications networks against cyber-attacks and new mobile networking protocols that afford resilience within our networks to automatically 'fight through' and/or evade hostile cyber effects.

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

Research in this Project is performed by the United States Army Futures Command (AFC).

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Cyber Security Applied Research & Experimentation Partner (AREP) Technology	2.785	-	-
Description: This effort will take innovative basic research theories from the Cyber Collaborative Research Alliance (CRA) and experimentally validate the hypothesis and create proof-of-concept defensive cyber software implementations.			
Accomplishments/Planned Programs Subtotals	2.785	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A