Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army											Date: May 2021	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 1: *Basic Research*					R-1 Program Element (Number/Name) PE 0601121A / *Cyber Collaborative Research Alliance*							
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	-	4.982	5.077	5.067	-	5.067	-	-	-	-	-	-
CB5: *Cyber Collaborative Research Alliance*	-	4.982	5.077	5.067	-	5.067	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

This PE fosters research performed through the Cyber Security Collaborative Research Alliance (CSEC CRA), a competitively selected consortium, formed to advance the theoretical foundations of cyber science in the context of Army networks. This CRA consists of academia, industry and government researchers working jointly with the objective of developing a fundamental understanding of cyber phenomena so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. This research focuses on three interrelated aspects of cyber security and is conducted using a trans-disciplinary approach that takes into account the human element of the network. The three aspects of cyber that are addressed are: 1) vulnerabilities and risks of cyber networks to malicious activities, 2) anticipating, detecting, and analyzing malicious activities, and 3) agile cyber maneuver to thwart and defeat malicious activities. Overarching goals of cyber security are to significantly decrease the adversary's return on investment when considering cyber attack on Army networks, and minimizing the impact on (Army) network performance related to implementing cyber security. The CRA research creates a framework that effectively integrates the knowledge of cyber assets and potential adversary capabilities and approaches, and provides defense mechanisms that dynamically adjust to changes related to mission, assets, vulnerability state, and defense mechanisms.

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

All FY20 adjustments align program financial structure to Army Modernization Priorities in support of the National Defense Strategy.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	4.982	5.077	5.181	-	5.181
Current President's Budget	4.982	5.077	5.067	-	5.067
Total Adjustments	0.000	0.000	-0.114	-	-0.114
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-0.114	-	-0.114

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 1	R-1 Program Element (Number/Name) PE 0601121A / *Cyber Collaborative Research Alliance*	Project (Number/Name) CB5 / *Cyber Collaborative Research Alliance*	

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
CB5: *Cyber Collaborative Research Alliance*	-	4.982	5.077	5.067	-	5.067	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

This Project fosters research performed through the Cyber Security Collaborative Research Alliance (CSEC CRA), a competitively selected consortium, formed to advance the theoretical foundations of cyber science in the context of Army networks. This CRA consists of academia, industry, and government researchers working jointly to develop a fundamental understanding of cyber phenomena so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. This research focuses on three interrelated aspects of cyber security and is conducted using a trans-disciplinary approach that takes into account the human element of the network. The three aspects of cyber that are addressed are: 1) adaptive reasoning for deception, 2) anticipating, detecting, and analyzing malicious activities, and 3) agile cyber maneuver to thwart and defeat malicious activities. Overarching goals of cyber security are to significantly decrease the adversary's return on investment when considering cyber attack on Army networks, and minimizing the impact on (Army) network performance related to implementing cyber security. The CRA research creates a framework that effectively integrates the knowledge of cyber assets and potential adversary capabilities and approaches, and provides defense mechanisms that dynamically adjust to changes related to mission, assets, vulnerability state, and defense mechanisms.

The cited work is consistent with the Assistant Secretary of Defense, Research and Engineering Science and Technology focus areas and the Army Modernization Strategy.

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyber Security Collaborative Research Alliance	4.982	5.077	5.067
Description: The CSEC CRA supports basic research to enable capabilities for rapid development and adaptation of cyber tools for dynamically assessing cyber risks, detecting hostile activities on friendly networks, and supporting agile maneuver in cyber space in spite of the emergence of novel threats.			
FY 2021 Plans: Investigate theories and models for reasoning about adversarial intent, defeating enemy Artificial Intelligence (AI), and employing deception to protect networks and forces; create techniques for autonomous planning and control of cyber maneuvers to deceive adversaries and protect networks; study methods for intelligent cyber threat detection and recognition in complex, adversarial and uncertain environments.			
FY 2022 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 1	**R-1 Program Element (Number/Name)** PE 0601121A / *Cyber Collaborative Research Alliance*	**Project (Number/Name)** CB5 / *Cyber Collaborative Research Alliance*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Will investigate theories and models that study fundamental properties and capabilities of adaptive, scalable, and robust cyber threat detection techniques; investigate methods for planning, assessing, and directing autonomous cyber maneuvers; research fundamental properties and capabilities of adaptive deception techniques for cyber defense, mission resilience, and counter-adversarial machine learning, in congested and contested tactical environments. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funding change reflects planned lifecycle of this effort.			
Accomplishments/Planned Programs Subtotals	4.982	5.077	5.067

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A