Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army											Date: March 2024	
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 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	-	5.355	5.459	5.525	-	5.525	5.532	5.536	5.596	5.652	0.000	38.655
CB5: *Cyber Collaborative Research Alliance*	-	5.355	5.459	5.525	-	5.525	5.532	5.536	5.596	5.652	0.000	38.655

A. Mission Description and Budget Item Justification

This Program Element (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.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	5.355	5.459	5.514	-	5.514
Current President's Budget	5.355	5.459	5.525	-	5.525
Total Adjustments	0.000	0.000	0.011	-	0.011
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	0.011	-	0.011

Change Summary Explanation

Minor increase in FY25 funding from the previous PB to the current PB due to economic assumptions.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
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 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
CB5: *Cyber Collaborative Research Alliance*	-	5.355	5.459	5.525	-	5.525	5.532	5.536	5.596	5.652	0.000	38.655

A. Mission Description and Budget Item Justification

This Project fosters cyber research, performed by a competitively selected consortium, formed to advance the theoretical foundations of cyber science in the context of Army networks. This work 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 cyber aspects 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. The overarching goals 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. This 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 Army Research Laboratory (ARL).

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Cyber Security Collaborative Research Alliance ***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.	5.355	-	-
Title: Adversarial-resilient Cyber Effects for Decision Dominance ***Description:*** Conduct foundational research to create innovative theories, models, and methods to understand, create, predict, and exploit Windows of Superiority (WoS) across the cyberspace-network to achieve operational advantage for Multi-Domain Operations (MDO) synchronization and convergence across domains. This effort seeks to identify, formalize, and measure the key attributes/features in the cyber domain that can identify and predict WoS. This effort will develop theories and methods to identify and predict emerging WoS and techniques to shape the cyber domain to achieve WoS, including cyber resilience and deception to mitigate adversarial deception, intrusions, and adversarial machine learning (AML) attacks.	-	5.459	5.525

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
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 2023	FY 2024	FY 2025
FY 2024 Plans: Will create an initial formalization for defining and reasoning about cyber domain Windows of Superiority; investigate methodologies to identify and exploit information from the network, network intrusion detection systems, information assets, and intelligence needed to assess cyber-network state and characterize a Window of Superiority in the cyber domain; develop techniques to detect adversarial deception in the cyber domain; explore techniques to provide cyber resilience for machine learning based algorithms for intrusion detection and network state estimation. ***FY 2025 Plans:*** Will conduct research into methodologies to identify, predict, reason, create, and exploit cyber security Windows of Superiority; explore techniques to enable multidomain cyber deception in contested environments; explore techniques to counter adversarial attacks and manipulation of machine learning based algorithms utilized for network defenses; examine impact of uncertainties and incomplete information in machine learning algorithms for cyber deception and network intrusion detection. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** Funding increase due to economic assumptions.			
Accomplishments/Planned Programs Subtotals	5.355	5.459	5.525

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A