

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army										Date: March 2019		
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	0.000	0.000	4.982	-	4.982	5.082	5.186	5.290	5.349	0.000	25.889
CB5: Cyber Collaborative Research Alliance	-	0.000	0.000	4.982	-	4.982	5.082	5.186	5.290	5.349	0.000	25.889

Note

In Fiscal Year (FY) 2020 this Program Element (PE) was previously funded, with continuity of effort realigned from the following PE:
 * PE 0601104A University and Industry Research Centers

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.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army					Date: March 2019
Appropriation/Budget Activity 2040: <i>Research, Development, Test & Evaluation, Army / BA 1: Basic Research</i>			R-1 Program Element (Number/Name) PE 0601121A / <i>Cyber Collaborative Research Alliance</i>		
B. Program Change Summary (\$ in Millions)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	0.000	0.000	0.000	-	0.000
Current President's Budget	0.000	0.000	4.982	-	4.982
Total Adjustments	0.000	0.000	4.982	-	4.982
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	4.982	-	4.982
 <u>Change Summary Explanation</u> FY20 funding increase adjustments related to Science and Technology Financial Restructuring.					

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army										Date: March 2019		
Appropriation/Budget Activity 2040 / 1					R-1 Program Element (Number/Name) PE 0601121A / <i>Cyber Collaborative Research Alliance</i>				Project (Number/Name) CB5 / <i>Cyber Collaborative Research Alliance</i>			
COST (\$ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
CB5: <i>Cyber Collaborative Research Alliance</i>	-	0.000	0.000	4.982	-	4.982	5.082	5.186	5.290	5.349	0.000	25.889

Note

In Fiscal Year (FY) 2020 this Project was realigned from:
Program Element (PE) 0601104A (University and Industry Research Centers)
* EA6 Cyber Collaborative Research Alliance

A. Mission Description and Budget Item Justification

This Project fosters research performed through the 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.

Work in this Project supports key Army needs and provides the technical underpinnings to PE 0602146A Network C3I Technology.

FY20 realignments are due to financial restructuring in support of Army Modernization Priorities.

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

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2018	FY 2019	FY 2020
Title: Cyber Security Collaborative Research Alliance	-	-	4.982
Description: The Cyber Security Collaborative Research Alliance (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 2020 Plans:			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army		Date: March 2019	
Appropriation/Budget Activity 2040 / 1	R-1 Program Element (Number/Name) PE 0601121A / <i>Cyber Collaborative Research Alliance</i>	Project (Number/Name) CB5 / <i>Cyber Collaborative Research Alliance</i>	
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2018	FY 2019
<p>Will model distributed, dynamic, secure coalition communication/information infrastructures that support distributed analytics to derive situational understanding; develop techniques for dynamic self-configuring services "on demand" based on mission needs, context and resource constraints; model underlying distributed analytics and situational understanding that supports dynamic coalition operations involving complex multi-actor situations.</p> <p><i>FY 2019 to FY 2020 Increase/Decrease Statement:</i> This research effort was realigned from PE 0601104A (University and Industry Research Centers) / Project EA6 (Cyber Collaborative Research Alliance) in FY20.</p>			
Accomplishments/Planned Programs Subtotals		-	4.982
C. Other Program Funding Summary (\$ in Millions)			
N/A			
Remarks			
D. Acquisition Strategy			
N/A			
E. Performance Metrics			
N/A			