Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Army	Date: March 2024
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0606942A *I Assessments and Evaluations Cyber Vulnerabilities*

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	-	5.816	6.025	10.105	-	10.105	6.372	6.441	6.512	6.577	Continuing	Continuing
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	5.816	6.025	10.105	-	10.105	6.372	6.441	6.512	6.577	Continuing	Continuing

A. Mission Description and Budget Item Justification

This funding line reduces the Army's risk to adversarial cyber intrusions or attacks that could compromise critical weapon systems and kill chains.

Cyberspace Operational-Resilience Assessment - Platform (CORA-P) improves survivability across Army modernization efforts and maintains readiness of operational capabilities. CORA-P addresses the requirements of Section 1647 of the FY16 NDAA and Section 1712 of the FY21 NDAA, which directs the Services to identify and mitigate cyberspace vulnerabilities in critical weapon systems. Under CORA-P, the Army prioritizes capabilities most-relevant to JROC-designated and threat-informed capabilities supporting National Defense Strategy priorities. The Army reviews the security posture of these critical components, develops remediation strategies, and facilitates delivery of fixes at mission-relevant speed. CORA-P is helping move the Army from system-oriented compliance to system-of-systems resilience that addresses defensive gaps between individual components; this is necessary to prevent adversaries from denying critical kill chains. CORA-P ensures Army cyberspace remediation investments address areas of highest operational risk.

When applicable, this PE also provides for Red Team enhancement to support Combatant Command mission-level cyber vulnerability assessments.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	5.816	6.025	6.185	-	6.185
Current President's Budget	5.816	6.025	10.105	-	10.105
Total Adjustments	0.000	0.000	3.920	-	3.920
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	3.920	-	3.920

Change Summary Explanation

The funding increase represents the addition of The Army Acquisition Red Team capabilities. The Army Acquisition Red Team provides Threat Counter Artificial Intelligence (TCAI) capability to test emerging and evolving DoD/Army AI and Machine Learning capabilities against relevant threats.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army			Date: March 2024
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0606942A / *Assessments and Evaluations Cyber Vulnerabilities*	Project (Number/Name) FL2 / *Cyber Vulnerabilities Assessments and Evaluations*	

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
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	5.816	6.025	10.105	-	10.105	6.372	6.441	6.512	6.577	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This funding line reduces the Army's risk to adversarial cyber intrusions or attacks that could compromise critical weapon systems and kill chains.

Cyberspace Operational-Resilience Assessment - Platform (CORA-P) improves survivability across Army modernization efforts and maintains readiness of operational capabilities. CORA-P addresses the requirements of Section 1647 of the FY16 NDAA, which directed the Services to identify and mitigate cyberspace vulnerabilities in critical weapon systems. The Army initially established CORA-P to continue Section 1647 assessments, while expanding to include supply chain risk analysis, electromagnetic spectrum vulnerabilities, persistent cyber red teaming, and crosscutting/architectural vulnerabilities. CORA-P now integrates with and enhances the DoD's Strategic Cybersecurity Program, as enacted in Section 1712 of the FY21 NDAA. Accordingly, CORA-P is shifting from executing new assessments, to developing and delivering vulnerability remediations from ongoing assessments and defensive operations. This includes improving the structure and visibility of vulnerability data to improve portfolio risk management, initiating remediation efforts for high-priority, crosscutting issues, and avoiding future risks by driving improvements earlier in materiel development for modernization programs.

Under CORA-P, the Army prioritizes capabilities most-relevant to JROC-designated and threat-informed capabilities supporting National Defense Strategy priorities. The Army reviews the security posture of these critical components, develops remediation strategies, and facilitates delivery of fixes at mission-relevant speed. CORA-P is helping move the Army from system-oriented compliance to system-of-systems resilience that addresses defensive gaps between individual components; this is necessary to prevent adversaries from denying critical kill chains. CORA-P ensures Army cyberspace remediation investments address areas of highest operational risk. CORA-P also provides the framework by which individual programs can elevate threat-informed remediation requirements to drive cybersecurity investments across portfolios to mission areas of highest operational risk.

When applicable, this PE also provides for Red Team enhancement to support Combatant Command mission-level cyber vulnerability assessments.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Cyberspace Operational Resiliency Assessment - Platform (CORA-P)	5.816	6.025	6.197
Description: CORA-P is the Army's response to Section 1647 of the 2016 National Defense Authorization Act which directed the Department of the Defense (DoD) to evaluate cyber vulnerabilities of major weapon systems. HQ Department of the Army Cyber Directorate will be the oversight governing body overseeing the assessments and NRE mitigations process to cyber vulnerabilities identified in the Vulnerability Assessment Report.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 6	**R-1 Program Element (Number/Name)** PE 0606942A / *Assessments and Evaluations Cyber Vulnerabilities*	**Project (Number/Name)** FL2 / *Cyber Vulnerabilities Assessments and Evaluations*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
FY 2024 Plans: The funding provides the Army the opportunity to complete evaluation of critical Army platforms as a follow-on to Section 1647 of the 2016 National Defense Authorization Act (NDAA). This includes system-of-systems assessments, lab assessments, tabletop exercises, and additional analytical, exercise, and or operational assessments. This funding provides the Army the ability to develop Red Team capacity to carry out COCOM mission level assessments. Cyber hardening efforts will be informed by the Cyber Vulnerability Assessment Report (CVAR) generated through the assessment and prioritization process. Prioritization will be based on mission, impact to readiness, and threat analysis. ***FY 2025 Plans:*** The funding provides the Army the opportunity to assure its digital transformation through automation to improve efficiency and effectiveness of cyber vulnerability collection, analysis, and reporting to deliver resilient and survivable weapon systems. Improved automation will enable the analysis of products from engineering, Test & Evaluation, and other assessments to proactively identify areas of risk (e.g. compromised software, unsecure configurations, supply chain vulnerabilities, etc). Enhancements will be leveraged to develop specific remediation plans/actions for priority findings from the DoD Security Cooperation Program and other defensive cyberspace operations in order to deliver fixes at mission relevant speeds. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2024 to FY 2025 funding increase represents minor increase due to economic assumptions.			
Title: Red Team ***Description:*** The Army Acquisition Red Team will provide Threat Counter Artificial Intelligence (TCAI) capability to test emerging and evolving DoD/Army AI and Machine Learning (ML) capabilities against operationally relevant and realistic threats. TCAI is critical to testing Army modernization efforts and evaluation of how it will conduct Multi-Domain Operations. Army Acquisition Red Team provides Persistent Cyber Operations (PCO) at the COCOM mission level, develops adversary techniques, tactics, and procedures (TTPs), conducts broad assessments of Science and Technology (S&T) and acquisition office environments and industrial base assets, as well as support CORA-P function providing PCO, Close Access Assessments, and Adversarial Assessments in support of Section 1647 of the 2016 National Defense Authorization Act. ***FY 2025 Plans:*** The funding provides the Army the ability to further develop the TCAI capability to test emerging and evolving DoD/Army AI and ML capabilities against operationally relevant and realistic threats critical to testing Army modernization priorities. The Army Acquisition Red Team will also provide PCO at the Combatant Command (COCOM) mission level, develop adversary Tactics Techniques and Procedures (TTPs), conduct broad assessments of S&T and acquisition office environments and industrial base assets. The Army Acquisition Red Team will support CORA-P providing PCO, Close Access Assessments, and Adversarial Assessments. The Army Acquisition Red Team supports multiple goals of the Army Campaign Plan to support delivering Army	-	-	3.908

Exhibit R-2A, RDT&E Project Justification: PB 2025 Army		Date: March 2024
Appropriation/Budget Activity 2040 / 6	**R-1 Program Element (Number/Name)** PE 0606942A / *Assessments and Evaluations Cyber Vulnerabilities*	**Project (Number/Name)** FL2 / *Cyber Vulnerabilities Assessments and Evaluations*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
2030 by ensuring S&T and PM environments are censored and defending intellectual property and critical technology information, expanding persistent cyberspace operations on COCOM networks under Director, Operational Test & Evaluation (DOT&E) authorities, and ensuring the organic industrial base can meet OPTEMPO requirements and delivery uncompromised. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2024 to FY 2025 funding increase represents the addition of Acquisition Red Team capabilities.			
Accomplishments/Planned Programs Subtotals	5.816	6.025	10.105

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A