

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army **Date:** March 2023

Appropriation/Budget Activity 2040: <i>Research, Development, Test & Evaluation, Army / BA 6: RDT&E Management Support</i>	R-1 Program Element (Number/Name) PE 0606942A / <i>Assessments and Evaluations Cyber Vulnerabilities</i>
--	--

COST (\$ in Millions)	Prior Years	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
Total Program Element	-	5.466	5.816	6.025	-	6.025	6.185	6.360	6.428	6.499	0.000	42.779
FL2: <i>Cyber Vulnerabilities Assessments and Evaluations</i>	-	5.466	5.816	6.025	-	6.025	6.185	6.360	6.428	6.499	0.000	42.779

A. Mission Description and Budget Item Justification

This funding line supports testing of Army Modernization Priority Programs.

The National Defense Authorization Acts (NDAA), Fiscal Year (FY) 16 Section 1647, and FY 17 Section 1650, directs the office of the Secretary of Defense (OSD) to complete an evaluation of cyberspace vulnerabilities of select Department of Defense (DoD) weapon systems and critical infrastructures. For NDAA 1647, the Army was directed to assess and mitigate twenty-four weapon systems not later than December 31, 2019. For NDAA 1650, the Army was directed to assess and submit a mitigation strategy for twenty-five installations by December 31, 2020. To support this mandate, the two Congressional mandates were merged into two enduring Army programs: the Cyber Operational Resiliency Assessment-Platforms (CORA-P) to replace NDAA 1647, and the Cyber Operational Resiliency Assessment-Installations (CORA-I) to replace NDAA 1650. The aim of CORA-P/I is to reduce the Army's risk to adversarial cyber intrusions or attacks that compromise Army weapon and installation systems. Performance objective is to provide governance oversight of CORA-P/I phased vulnerability assessments to support the Planning, Programming, Budgeting and Execution (PPBE) cycle. These deliverables include identifying the means to mitigate CORA-P/I vulnerabilities.

Efforts in this Program Element will: 1) identify, assess, and develop non-recurring engineering (NRE) to mitigate operational risks from cyber vulnerabilities to critical Army weapon systems in an operational configuration; and 2) assure the confidentiality, availability, and integrity of the information and control systems that underpin Army facilities and critical infrastructure by inventorying and assessing Facility-Related Control Systems (FRCS).

Weapon systems evaluations will assess and provide NRE recommendations to mitigate operational risks emanating from a peer or near-peer adversary profile in accordance with existing test/lab requirements through the acquisition cycle. Where applicable, these evaluations will include tabletop exercises, lab assessments, and exercise/operational assessments of Program Executive Officer Command, Control, Communications-Tactical (PEO C3T) and ground weapon systems. Cyber hardening efforts will be informed by the vulnerability assessments reports (VAR) generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat. When applicable, this PE also provides for Red Team enhancement to support Combatant Command mission-level cyber vulnerability assessments.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army	Date: March 2023
---	-------------------------

Appropriation/Budget Activity 2040: <i>Research, Development, Test & Evaluation, Army / BA 6: RDT&E Management Support</i>	R-1 Program Element (Number/Name) PE 0606942A / <i>Assessments and Evaluations Cyber Vulnerabilities</i>
--	--

B. Program Change Summary (\$ in Millions)	<u>FY 2022</u>	<u>FY 2023</u>	<u>FY 2024 Base</u>	<u>FY 2024 OCO</u>	<u>FY 2024 Total</u>
Previous President's Budget	5.466	5.816	5.998	-	5.998
Current President's Budget	5.466	5.816	6.025	-	6.025
Total Adjustments	0.000	0.000	0.027	-	0.027
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	0.027	-	0.027

Change Summary Explanation

Increased funding due to revised economic assumptions.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army										Date: March 2023		
Appropriation/Budget Activity 2040 / 6					R-1 Program Element (Number/Name) PE 0606942A / <i>Assessments and Evaluations Cyber Vulnerabilities</i>				Project (Number/Name) FL2 / <i>Cyber Vulnerabilities Assessments and Evaluations</i>			
COST (\$ in Millions)	Prior Years	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
FL2: <i>Cyber Vulnerabilities Assessments and Evaluations</i>	-	5.466	5.816	6.025	-	6.025	6.185	6.360	6.428	6.499	0.000	42.779
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project funds cyber vulnerabilities evaluations of major weapon systems in alignment with Section 1647 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, and of critical infrastructure in alignment with Section 1650 of NDAA FY 2017. Efforts in this Project will: 1) identify, assess, and develop and identify non-recurring engineering (NRE) to mitigate operational risks from cyber vulnerabilities to critical Army weapon systems in an operational configuration; and 2) assure the confidentiality, availability, and integrity of the information and control systems that underpin Army facilities and critical infrastructure by inventorying and assessing Facility-Related Control Systems (FRCS).

Weapon systems evaluations will assess and provide NRE recommendations to mitigate operational risks emanating from a peer or near-peer adversary profile in accordance with existing test/lab requirements through acquisition cycle. Where applicable, these evaluations will include tabletop exercises, lab assessments, and exercise/operational assessments of Program Executive Officer Command, Control, Communications-Tactical (PEO C3T) and ground weapon systems. Cyber hardening efforts will be informed by the vulnerability assessments reports (VAR) generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat. 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 2022	FY 2023	FY 2024
Title: Cyberspace Operational Resiliency Assessment - Platform (CORA-P)	2.733	5.816	6.025
Description: CORA-P is the Army's response to Section 1647 of the 2016 National Defense Authorization Act (NDAA) which directed the Department of the Defense (DoD) to evaluate cyber vulnerabilities of major weapon systems. HQ Department of the Army Cyber Directorate (DAMO-CY) will be the oversight governing body overseeing the assessments and NRE mitigations process to cyber vulnerabilities identified in the VAR.			
FY 2023 Plans:			
The funding provides ASA(ALT) the opportunity to complete evaluation of critical Army platforms identified by the Army G 3/5/7 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 ASA(ALT) 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			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023		
Appropriation/Budget Activity 2040 / 6	R-1 Program Element (Number/Name) PE 0606942A / <i>Assessments and Evaluations Cyber Vulnerabilities</i>	Project (Number/Name) FL2 / <i>Cyber Vulnerabilities Assessments and Evaluations</i>		
B. Accomplishments/Planned Programs (\$ in Millions)		FY 2022	FY 2023	FY 2024
<p>prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat analysis as determined by the Army G 3/5/7 and Army Cyber Council of Colonels.</p> <p>FY 2024 Plans: The funding provides ASA(ALT) the opportunity to complete evaluation of critical Army platforms identified by the Army G 3/5/7 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 ASA(ALT) 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 criticality, impact to readiness, and threat analysis as determined by the Army G 3/5/7 and Army Cyber Council of Colonels.</p> <p>FY 2023 to FY 2024 Increase/Decrease Statement: Funding increase supports the planned lifecycle of the effort.</p>				
<p>Title: Cyberspace Operational Resiliency Assessment - Installation (CORA-I)</p> <p>Description: CORA-I is the Army's response to Section 1650 of the 2017 NDAA. Evaluations of cyber vulnerabilities to critical infrastructure will focus on Task Critical Assets, Defense Critical Assets, and on units with high priority Quadrennial Defense Review missions and their supporting infrastructure. When necessary, this PE will provide for the training of teams to conduct cyber vulnerability evaluations on critical infrastructure. Once trained, these teams will conduct cooperative vulnerability and penetration assessments (Blue Teaming), adversarial assessments (Red Teaming), and assist with conducting assessments of cyber dependencies, vulnerabilities and threats in accordance with DoDI 8501.1 "Risk Management Framework." Funding will also provide for Contractor subject matter expertise to conduct Security Control Assessments and Deep Cyber Resiliency Assessments.</p>		2.733	-	-
Accomplishments/Planned Programs Subtotals		5.466	5.816	6.025
C. Other Program Funding Summary (\$ in Millions)				
N/A				
Remarks				
D. Acquisition Strategy				
N/A				