Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army											Date: April 2022	
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 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**Cost To Complete**	**Total Cost**
Total Program Element	-	6.496	5.466	5.816	-	5.816	5.998	6.150	6.319	6.381	0.000	42.626
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	6.496	5.466	5.816	-	5.816	5.998	6.150	6.319	6.381	0.000	42.626

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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army	Date: April 2022
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*

B. Program Change Summary ($ in Millions)	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total
Previous President's Budget	6.496	5.466	0.000	-	0.000
Current President's Budget	6.496	5.466	5.816	-	5.816
Total Adjustments	0.000	0.000	5.816	-	5.816
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	5.816	-	5.816

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2021	FY 2022
Project: FL2: *Cyber Vulnerabilities Assessments and Evaluations*		
Congressional Add: *Program increase - cyber vulnerability assessment*	2.000	-
Congressional Add Subtotals for Project: FL2	2.000	-
Congressional Add Totals for all Projects	2.000	-

Change Summary Explanation

FY 2023 funding increase reflects the fact that the FY 2022 President's Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	6.496	5.466	5.816	-	5.816	5.998	6.150	6.319	6.381	0.000	42.626
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 2021	FY 2022	FY 2023
Title: Cyberspace Operational Resiliency Assessment ? Platform (CORA-P)	2.248	2.733	5.816
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 2022 Plans: The funding provides DAMO-CY the opportunity to complete evaluation of the 24 critical weapon systems and the 26 critical infrastructures for cyber vulnerabilities, identified by the DoD, in support of NDAAs 1647 and 1650. This includes lab assessments, tabletop exercises, and additional analytical, exercise, and or operational assessments. This funding provides DAMO-CY the ability to develop Red Team capacity to carry out COCOM mission level assessments. Cyber hardening efforts will be informed by			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
the VAR generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat analysis. ***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 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. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** FY2022 to FY2023 increase is due to the amount of critical Army platforms tested from FY2022 to FY2023.			
Title: Cyberspace Operational Resiliency Assessment ? Installation (CORA-I) ***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. ***FY 2022 Plans:*** Funding provides for the completion of the select-DoD twenty-five critical infrastructures assessments already in some stage of the evaluation process, identified as part of the Section 1650 directive, executed through on-sight assessments. These assessments result in VAR in support of the Planning, Programming, Budgeting, and Execution (PPBE) cycle. Funding also provides developing and maintaining a Red and Blue teams carry out on-site assessments. Cyber hardening efforts will be informed by the VAR generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat. ***FY 2022 to FY 2023 Increase/Decrease Statement:***	2.248	2.733	-

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
FY 2022 to FY 2023 decrease in funding as CORA-I efforts are complete in FY 2022.			
Accomplishments/Planned Programs Subtotals	4.496	5.466	5.816

	FY 2021	FY 2022
Congressional Add: Program increase - cyber vulnerability assessment	2.000	-
FY 2021 Accomplishments: FY 2021 Congressional Add for Cyber Vulnerability Assessments for Red Teams.		
Congressional Adds Subtotals	2.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A