Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army												Date: May 2021
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
Total Program Element	-	4.500	6.496	5.466	-	5.466	-	-	-	-	-	-
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	4.500	6.496	5.466	-	5.466	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

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 2022 Army	Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	4.500	4.496	4.496	-	4.496
Current President's Budget	4.500	6.496	5.466	-	5.466
Total Adjustments	0.000	2.000	0.970	-	0.970
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	2.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	0.970	-	0.970

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2020	FY 2021
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 2021 increase allows for development of new analytic methodologies to make use of commercially available data that can be applied to military and Defense Industrial Base (DIB) targets to identify vulnerabilities in the cyber and physical supply chain or critical assets and facilities. The increase develops a process that allows for a comprehensive, intelligence informed assessment that can be applied to critical weapon systems and Combatant Commands (CCMDs) as well as the ecosystems that support them by providing a holistic look at cyber defense posture, resiliency, supply chain and development of cyber-electronic warfare (EW) convergence techniques.

FY 2022 increase allows for further development of new analytic methodologies to make use of commercially available data that can be applied to military and Defense Industrial Base (DIB) targets to identify vulnerabilities in the cyber and physical supply chain or critical assets and facilities.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	4.500	6.496	5.466	-	5.466	-	-	-	-	-	-
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 2020	FY 2021	FY 2022
Title: Cyberspace Operational Resiliency Assessment ? Platform (CORA-P)	-	2.248	2.733
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 2021 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 Combatant Command (COCOM) mission level assessments. Cyber hardening			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
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 analysis ***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 the VAR generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat analysis. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY 2021 to FY 2022 increase is due to the completion of the critical weapons systems and critical infrastructures for cyber vulnerabilities.			
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 2021 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 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 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	-	2.248	2.733

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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 2020	FY 2021	FY 2022
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 2021 to FY 2022 Increase/Decrease Statement:*** FY 2021 to FY 2022 increase for the analytic methodologies developed to use commercially available data used in prototype.			
Title: U.S. Army Corps of Engineer (USACE) Tiger Team ***Description:*** USACE Tiger Team conducts planning and scoping for the NDAA 1650 Mitigations.	0.098	-	-
Title: Mission Relevant Terrain-Cyber ***Description:*** Identification and Protection of Key Cyber Terrain in major commands.	0.451	-	-
Title: Secure Gray Eagle Maintenance Support ***Description:*** Provides Cyber Resilient Software Maintenance support to assure the readiness of Gray Eagle Unmanned Aerial System.	2.814	-	-
Title: Operations Support Cell ***Description:*** Weapons and infrastructure assessment schedulers and mitigation report writers.	0.794	-	-
Title: Boundary Layer Protection ***Description:*** Addresses the FY16 National Defense Authorization Act 1647 cyber assessments identified in developing a Boundary Layer Protection as one of the crosscutting areas of interest.	0.343	-	-
Accomplishments/Planned Programs Subtotals	4.500	4.496	5.466

	FY 2020	FY 2021
Congressional Add: Program increase - cyber vulnerability assessment ***FY 2021 Plans:*** FY 2021 Congressional Add for Cyber Vulnerability Assessments for Red Teams.	-	2.000
Congressional Adds Subtotals	-	2.000

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
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*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

N/A