Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army											Date: February 2020	
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 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
Total Program Element	-	88.300	4.500	4.496	-	4.496	4.496	4.496	4.676	4.723	0.000	115.687
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	88.300	4.500	4.496	-	4.496	4.496	4.496	4.676	4.723	0.000	115.687

A. Mission Description and Budget Item Justification

The National Defense Authorization Acts (NDAA), Fiscal Years (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 DoD weapon systems and critical infrastructures. For NDAA 1647, the Army was directed to assess and mitigate twenty-four weapon systems NLT December 31, 2019. For NDAA 1650, the Army was directed to assess and submit a mitigation strategy for twenty-five installations, NLT 31 December, 2020. To support this mandate, the HQDA G-3 directed DAMO-CY to evolve the two congressional mandates 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 compromises the Army weapon and installation systems. In compliance with the congressional mandates, DAMO-CY's performance objectives is to provide governance oversight over the execution of CORA-P/I phased vulnerability assessments to support o the Planning, Programming, Budgeting and Execution (PPBE) cycle. These deliverables include identifying the means to mitigate CORA-P/I vulnerabilities.

This Program Element (PE) 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 2017. Efforts in this PE 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 of 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.

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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	88.300	4.500	4.500	-	4.500
Current President's Budget	88.300	4.500	4.496	-	4.496
Total Adjustments	0.000	0.000	-0.004	-	-0.004
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-0.004	-	-0.004

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	88.300	4.500	4.496	-	4.496	4.496	4.496	4.676	4.723	0.000	115.687
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Program Element (PE) 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 2017. Efforts in this PE 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 of 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.

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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Cyberspace Operational Resiliency Assessment ? Platform (CORA-P)	37.450	2.250	2.248
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. DAMO-CY will be the oversight governing body overseeing the assessments and NRE mitigations process to cyber vulnerabilities identified in the VAR.			
FY 2020 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
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 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 analysis. ***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 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 analysis ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Nominal change in program.			
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 2020 Plans:*** Funding provides for the training of teams to conduct cyber vulnerability assessments 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 8510.1 "Risk Management Framework." Funding also provides for Contractor subject matter expertise to conduct Security Control Assessments and Deep Cyber Resiliency Assessments. The 2017 Army Cybersecurity Strategy for FRCS further established the requirement to inventory and conduct Risk Management Framework on select-DoD legacy systems. The Unified Facility	37.450	2.250	2.248

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021
Criteria 4-010-06 also established the requirement to design cybersecurity protections into FRCS within all new MILCON projects. 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. ***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 vulnerability assessments reports (VAR) generated through the assessment and prioritization process. Prioritization will be based on mission criticality, impact to readiness, and threat. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Nominal change in program.			
Title: Fiscal Year 2019 (FY19) Pending Recission ***Description:*** FY19 Pending Recission	13.400	-	-
Accomplishments/Planned Programs Subtotals	88.300	4.500	4.496

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A