Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army											Date: March 2019	
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 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**Cost To Complete**	**Total Cost**
Total Program Element	-	0.000	88.300	4.500	-	4.500	4.500	4.500	4.500	4.680	0.000	110.980
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	0.000	88.300	4.500	-	4.500	4.500	4.500	4.500	4.680	0.000	110.980

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 mitigate operational risk from cyber vulnerabilities as it pertains 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 mitigate operational risk from a peer or near-peer adversary profile in accordance with existing testing requirements of 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 apply knowledge from weapon systems vulnerability assessments to identify gaps and develop mitigation strategies to reduce operational risk and prioritize resources. Prioritization will be based on mission criticality, impact to readiness, and threat. This PE also provides for enhancement of existing Red Team elements and efforts attributed to Combatant Command mission-level cyber vulnerability assessments.

Evaluations of cyber vulnerabilities at 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. This PE provides 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 2020 Army					Date: March 2019
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 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**
Previous President's Budget	0.000	88.300	0.000	-	0.000
Current President's Budget	0.000	88.300	4.500	-	4.500
Total Adjustments	0.000	0.000	4.500	-	4.500
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	4.500	-	4.500

Change Summary Explanation

Fiscal Year (FY) 2020 funding is to continue conducting Cyberspace Operational Resiliency Assessments at both Platform and Installation levels (CORA-P/I).

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army			Date: March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
FL2: *Cyber Vulnerabilities Assessments and Evaluations*	-	0.000	88.300	4.500	-	4.500	4.500	4.500	4.500	4.680	0.000	110.980
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 2016, and of critical infrastructure in alignment with Section 1650 of NDAA 2017. Efforts in this PE will: 1) identify, assess, and mitigate operational risk from cyber vulnerabilities as it pertains 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 mitigate operational risk from a peer or near-peer adversary profile in accordance with existing testing requirements of 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 apply knowledge from weapon systems vulnerability assessments to identify gaps and develop mitigation strategies to reduce operational risk and prioritize resources. Prioritization will be based on mission criticality, impact to readiness, and threat. This PE also provides for enhancement of existing Red Team elements and efforts attributed to Combatant Command mission-level cyber vulnerability assessments.

Evaluations of cyber vulnerabilities at 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. First, this PE provides 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 2018	FY 2019	FY 2020
Title: Cyberspace Operational Resiliency Assessment ? Platform (CORA-P)	-	30.800	2.250
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. The effort will assess and mitigate operational risk from cyber vulnerabilities of major weapon systems from a peer or near-peer adversary profile in coordination with existing testing requirements of the acquisition cycle.			
FY 2019 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army		Date: March 2019
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 2018	FY 2019	FY 2020
Funding provides for the completion of the eight critical weapon systems already in some stage of the evaluation process. Additionally, provides for the 11 remaining Program Executive Officer Command, Control, Communications-Tactical (PEO C3T) and ground weapon systems identified as a part of the Section 1647 directive by conducting tabletop exercises, lab assessments, and exercise/operational assessments (where applicable). Provides for the enhancement of existing red team elements and efforts attributed to Combatant Command (COCOM) mission level assessments. Cyber hardening efforts will apply the knowledge from weapon systems vulnerability assessments (CORA-P) to identify the gaps, develop mitigation strategies to reduce operational risk and prioritize resources. Prioritization will be based on mission criticality, impact to readiness, and threat. ***FY 2020 Plans:*** The performance objectives is to conduct CORA-P vulnerability assessments and to produce the requisite vulnerability assessments reports in support of the Planning, Programming, and Budgeting and Execution (PPBE) cycle. These deliverables include extensive cyber tabletop exercises and other non-operational activities to identify precisely cyber threats that pose a risk to Army mission operations. Identifying cyber threats to CORA-P/I ensures that cyber survive-ability requirements are articulated sufficiently to ensure Army weapon systems and installations are designed/redesigned to prevent, mitigate and recover from adversarial current and future cyber-attacks. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 funding is to continue conducting CORA-P vulnerability assessments.			
Title: Cyberspace Operational Resiliency Assessment ? Installation (CORA-I) ***Description:*** CORA-I is the Army?s response to Section 1650 of the 2017 NDAA which directed the DoD to develop and execute a plan to evaluate and mitigate cyber vulnerabilities of Army Installations critical infrastructure. The evaluations will focus on Task Critical Assets, Defense Critical Assets, and on units with high priority Quadrennial Defense Review (QDR) missions and their supporting infrastructure. ***FY 2019 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.	-	57.500	2.250

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army		Date: March 2019
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 2018	FY 2019	FY 2020
The 2017 Army Cybersecurity Strategy for FRCS established the requirement to inventory and conduct Risk Management Framework on legacy systems. Concurrently, the Unified Facility Criteria 4-010-06 established the requirement to design cybersecurity protections into FRCS within all new MILCON projects. The cyber hardening efforts will apply the knowledge from critical installation vulnerability assessments (CORA-I) to identify the gaps, develop mitigation strategies to FRCS, and prioritize resources. Prioritization will be based on mission criticality, impact to readiness, and threat. ***FY 2020 Plans:*** The performance objectives is to conduct CORA-I vulnerability assessments and to produce the requisite vulnerability assessments reports in support of the PPBE cycle. These deliverables include extensive cyber tabletop exercises and other non-operational activities to identify precisely cyber threats that pose a risk to Army mission operations. Identifying cyber threats to CORA-P/I ensures that cyber survive-ability requirements are articulated sufficiently to ensure Army weapon systems and installations are designed/redesigned to prevent, mitigate and recover from adversarial current and future cyber-attacks. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY20 funding is to continue conducting CORA-I vulnerability assessments.			
Accomplishments/Planned Programs Subtotals	-	88.300	4.500

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A