Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army											Date: April 2022	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 6: *RDT&E Management Support*					R-1 Program Element (Number/Name) PE 0604256A / *Threat Simulator Development*							
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	-	41.487	61.422	18.437	-	18.437	11.581	15.550	11.533	11.645	0.000	171.655
976: *Army Threat Sim (ATS)*	-	41.487	61.422	18.437	-	18.437	11.581	15.550	11.533	11.645	0.000	171.655

A. Mission Description and Budget Item Justification

This funding line supports testing of Army Modernization Priority Programs.

This Program Element (PE) supports the design, development, acquisition, integration and fielding of realistic mobile threat simulators and realistic threat simulation products utilized in Army/Department of Defense (DoD) training and developmental and operational tests. This PE originally funded simulators representing Soviet equipment, but scope was expanded to address emerging world threats. Army Threat Simulator and Threat Simulation products are utilized to populate test battlefields for United States (U.S.) Army Test and Evaluation Command (ATEC), to conduct developmental and operational tests, and to support Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) required user testing in System Integration Laboratories (SILs) and hardware/simulation in-the-loop facilities. These battlefield simulators represent adversary systems (e.g. missile systems, command, control and communications systems, electronic warfare systems, etc.) in order to portray a realistic threat environment during testing of U.S. weapon systems.

Army Threat Simulator and Threat Simulation products developed or fielded under this PE support Army-wide, non-system-specific threat product requirements. Each capability is pursued in concert and coordination with existing Army/DoD and Tri-Service capabilities to eliminate duplication of effort. Simulator development is responsive to Office of the Secretary of Defense and Government Accountability Office guidance for the Army to conduct operational testing in a realistic threat environment. Actual threat equipment is acquired when appropriate (in lieu of development) and total package fielding is still required (i.e., instrumentation, operations and maintenance, manuals, new equipment training, etc.). Threat simulator development is accomplished under the auspices of the Project Manager for Cyber Test and Training (PM CT2) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

B. Program Change Summary ($ in Millions)	**FY 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**
Previous President's Budget	41.486	18.439	0.000	-	0.000
Current President's Budget	41.487	61.422	18.437	-	18.437
Total Adjustments	0.001	42.983	18.437	-	18.437
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	43.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	0.001	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	18.437	-	18.437

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 0604256A *I Threat Simulator Development*		
• FFRDC Transfer	-	-0.017	-	-	-

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2021	FY 2022
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Threat Cyberspace Operations*	3.750	3.000
Congressional Add: *Cyber Security Operations Center*	20.000	40.000
Congressional Add: *Cyber Threat Vulnerabilities & Assessments*	3.750	-
Congressional Add Subtotals for Project: 976	27.500	43.000
Congressional Add Totals for all Projects	27.500	43.000

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 0604256A / *Threat Simulator Development*	Project (Number/Name) 976 / *Army Threat Sim (ATS)*	

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
976: *Army Threat Sim (ATS)*	-	41.487	61.422	18.437	-	18.437	11.581	15.550	11.533	11.645	0.000	171.655
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This Project supports the design, development, acquisition, integration, and fielding of realistic mobile threat simulators and realistic threat simulation products utilized in Army/Department of Defense (DoD) training and developmental and operational tests. This Project originally funded simulators representing Soviet equipment, but scope was expanded to address emerging world threats. Army Threat Simulator and Threat Simulation products are utilized to populate test battlefields for the United States (U.S.) Army Test and Evaluation Command (ATEC), to conduct developmental and operational tests, and to support Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) required user testing in System Integration Laboratories (SILs) and hardware/simulation in-the-loop facilities. These battlefield simulators represent adversary systems (e.g. missile systems, command, control and communication systems, electronic warfare systems, etc.) in order to portray a realistic threat environment during testing of U.S. weapon systems.

Army Threat Simulator and Threat Simulation products developed or fielded under this Project support Army-wide, non-system-specific threat product requirements. Each capability is pursued in concert and coordination with existing Army/DoD and Tri-Service capabilities to eliminate duplication of effort. Simulator development is responsive to Office of the Secretary of Defense and Government Accountability Office guidance for the Army to conduct operational testing in a realistic threat environment. Actual threat equipment is acquired when appropriate (in lieu of development) and total package fielding is still required (i.e., instrumentation, operations and maintenance, manuals, new equipment training, etc.) Threat simulator development is accomplished under the auspices of the Project Manager for Cyber Test and Training (PM CT2) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Threat Information Warfare	4.805	5.753	5.813
Description: Provides cyber red team personnel and Information Operations (IO) weapons, Command and Control (C2), infrastructure, and research for advanced threat capabilities targeting Army programs, systems, and commands. Provides funds for cyber training and certifications of on-net interactive operators, certified ethical hackers, mission leads, planners and logistics. Access to real-time Internet flow information used for characterization of near-peer threats and the application of this information to Army targets.			
FY 2022 Plans: Continue to identify mission sets with focus on the integration of Red Team operator capabilities into the Threat Environments mission set, i.e. provide not only integration of red assets but also include threat defense, threat blue teams, and general threat-based CND operations. Operationalize NETT infrastructure and capabilities into a distributed cloud-based model such that other DoD Red Teams (joint teams) and Army teams can leverage the capability from geographically separated locations (fully			

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 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
distributed operations). Will develop state and non-state threat targeting packages that are current, accurately profiling attack trends and timelines, intent, levels of sophistication, and threat training. These threat packages represent state and non-state level forces using both active and passive network attack to selectively degrade or disrupt Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (C4ISR) and Enterprise Business Systems. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2023 Plans:*** Continue to identify mission sets with focus on the integration of Red Team operator capabilities into the Threat Environments mission set, i.e. provide not only integration of red assets but also include threat defense, threat blue teams, and general threat based Cyber Network Defense (CND) operations. Expand Network Exploitation Test Tool (NETT) infrastructure and capabilities into a distributed cloud-based model such that other DoD Red Teams (joint teams) and Army teams can leverage the capability from geographically separated locations (fully distributed operations). Will develop state and non-state threat targeting packages that are current, accurately profiling attack trends and timelines, intent, levels of sophistication, and threat training. These threat packages represent state and non-state level forces using both active and passive network attack to selectively degrade or disrupt Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (C4ISR) and Enterprise Business Systems. Development of threat targets and networks as new real-world targets sets and capabilities evolve. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Funding increase from FY 2022 to FY 2023 for hardware cost increases required for threat capability development. FY 2022 FFRDC reduction of $6K.			
Title: Threat Electronic Warfare	4.178	7.721	8.444
Description: Develops Army threat Electronic Warfare (EW) capabilities that will simulate a realistic anti-access/aerial denial (A2/AD) environment that will portray critical threats to U.S. DoD satellite communication (SATCOM), navigation, and command, control, and communication (C3I) networks. Develops specific EW capabilities to include cyber/EW convergence, tailored jamming in a complex radio frequency (RF) environment, data spoofing, detection of Low Probability Intercept (LPI) waveforms, artificial intelligence (AI), network modeling, passive detection systems, and advanced electronic support systems. The Threat Operations program will fund the operation, maintenance, management, and sustainment capability for Threat systems used to portray a realistic threat environment during Army testing and training within the Army's Threat inventory in order to support multiple Army/Department of Defense (DoD) test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous SUTs / PORs. ***FY 2022 Plans:*** Continue to develop and integrate electronic support sensors and electronic attack payloads to provide a robust and threat representative capability to support testing of Army systems. Threat Position, Navigation, and Timing (PNT) Jammer will consist			

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 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
of modifications and upgrades to ensure relevance by implementing additional capabilities within the PNT spectrum. Threat Operations will continue to support multiple Army test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test/ Programs of Record (SUT / POR) currently identified through FY2022. ***FY 2023 Plans:*** Continue to develop and integrate electronic support sensors and electronic attack payloads to provide a robust and threat representative capability to support testing of Army systems. Threat Position, Navigation, and Timing (PNT) Jammer will consist of modifications and upgrades to ensure relevance by implementing additional capabilities within the PNT spectrum. Threat Systems Management Office will continue to support multiple Army test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test/ Programs of Record (SUT / POR) currently identified through FY2023. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** FY 2023 increase will enable the Threat Systems Management Office (TSMO) to continue supporting multiple Army test events including Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test/ Programs of Record (SUT / POR) currently identified through FY2023. FY 2022 FFRDC reduction of $6K.			
Title: Threat Network and Mission Command ***Description:*** Develops Army threat Network and Mission Command capabilities to include quantum computing techniques, use of adaptive RF transmissions, self-healing/mesh network, capabilities aimed at masking threat communication systems (Very High Frequency (VHF), Ultra High Frequency (UHF), and High Frequency (HF), satellite and cellular, and next generation tactical radios. ***FY 2022 Plans:*** Continue system integration and improve the network fidelity, as well as develop data fusion and artificial intelligence to provide improved decision aids to the Threat Force Commander. ***FY 2023 Plans:*** Continue system integration and improve the network fidelity, as well as, develop data fusion and artificial intelligence to provide improved decision aids to the Threat Force Commander. Continue to develop and integrate electronic support sensors and electronic attack payloads to provide a robust and threat representative capability to support testing of Army systems. Threat Position, Navigation, and Timing (PNT) Jammer will consist of modifications and upgrades to ensure relevance by implementing additional capabilities within the PNT spectrum. Threat Operations will continue to support multiple Army test events including	5.004	4.275	4.180

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 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Joint Warfighting Assessment (JWA) and anticipated excursion test events for numerous Systems Under Test/ Programs of Record (SUT / POR) currently identified through FY2023. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Army decreased funding in FY 2023 due to higher Army priorities. FY 2022 FFRDC reduction of $5K.			
Title: SBIR/STTR ***FY 2022 Plans:*** Funding transferred in accordance with Title 15 USC ?638. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Funding transferred in accordance with Title 15 USC ?638.	-	0.673	-
Accomplishments/Planned Programs Subtotals	13.987	18.422	18.437

	FY 2021	FY 2022
Congressional Add: Threat Cyberspace Operations ***FY 2021 Accomplishments:*** Support of Cyber Threat and vulnerability assessments through the enhancement of Cyber Threat simulators, including the research and development of cyber security solutions (tools, techniques, tactics & procedures). ***FY 2022 Plans:*** Support to Cyber Threat and vulnerability assessments through the enhancement of Cyber Threat simulators, including the research and development of cyber security solutions (tools, techniques, tactics & procedures). Provides cyber red team Information Operations (IO) weapons, Command and Control (C2) infrastructure, and research for advanced threat capabilities targeting Army programs, systems, and commands. Furthers efforts executed under FY21 185 $3,750K Program Increase ?Threat Simulator Development?	3.750	3.000
Congressional Add: Cyber Security Operations Center ***FY 2021 Accomplishments:*** Continue the Cyber Security Operations Center (CSOC) technical capabilities by engaging a variety of Defense Industrial Base (DIB) participants to conduct multiple prototype demonstrations. Continue gathering data to conduct the feasibility assessment of providing scalable cyber security expertise to the DIB. Develop and demonstrate the ability to provide secure real-time cyber support to a series of cloud enabled customer bases. ***FY 2022 Plans:*** Prototype capability to evaluate the feasibility of providing cyber security services and expertise to the Defense Industrial Base (DIB). Refine techniques for providing on-site and remote DIB assistance with assessment, training, response, and mitigation of cyber vulnerabilities and industrial supply chains. Continue	20.000	40.000

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 0604256A / *Threat Simulator Development*	**Project (Number/Name)** 976 / *Army Threat Sim (ATS)*

	FY 2021	FY 2022
development and refinement of the ability to provide effective and secure real-time cyber support to a series of cloud-enabled distributed, or deployed government and/or industry customer bases. The FY 2022 Congressional Add funds will significantly increase the scale of support into the next phase of the prototype, which includes a drastically larger magnitude of DIB participants than executed in previous phases.		
Congressional Add: Cyber Threat Vulnerabilities & Assessments ***FY 2021 Accomplishments:*** TSMO is chartered as the threat provider for the Army Acquisition community and provides Red Team capabilities to all branches of the DoD. As such, TSMO has a responsibility to continuously develop new and maintain existing threat capabilities, in the cyber, physical, intelligence, and EW domains. Cyber Vulnerability Assessments (CVA) allow TSMO to develop and test new capabilities in support of the Army Test and Evaluation, Cyber Operations Resiliency Assessment ? Platform (CORA-P), and Persistent Cyber Operation (PCO) missions. CVA will enable TSMO to more closely replicate advanced adversarial capabilities resulting in more threat faithful testing of critical Army weapon and information systems.	3.750	-
Congressional Adds Subtotals	27.500	43.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A