Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Army												Date: February 2018
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 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
Total Program Element	-	28.883	22.862	12.835	-	12.835	15.284	15.544	16.014	16.403	0.000	127.825
976: *Army Threat Sim (ATS)*	-	28.883	22.862	12.835	-	12.835	15.284	15.544	16.014	16.403	0.000	127.825

A. Mission Description and Budget Item Justification

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 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 (PEO) required user testing in System Integration Laboratories 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 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 Instrumentation, Targets and Threat Simulators (PM ITTS) and the Director, Operational Test and Evaluation (DOT&E) Threat Simulator Investment Working Group.

Beginning in Fiscal Year 2019, this PE will also support the Advanced Electronic Support Sensor Suite (AESSS) and Cyber Blue Teams activities.

B. Program Change Summary ($ in Millions)	**FY 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**
Previous President's Budget	25.675	22.862	23.885	-	23.885
Current President's Budget	28.883	22.862	12.835	-	12.835
Total Adjustments	3.208	0.000	-11.050	-	-11.050
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	4.000	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.585	-			
• Adjustments to Budget Years	-0.200	-	-11.050	-	-11.050

Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Army				Date: February 2018
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	-0.007	-	-	-

Congressional Add Details ($ in Millions, and Includes General Reductions)

	FY 2017	FY 2018
Project: 976: *Army Threat Sim (ATS)*		
Congressional Add: *Congressional Add - Cyber Vulnerabilities*	4.000	-
Congressional Add Subtotals for Project: 976	4.000	-
Congressional Add Totals for all Projects	4.000	-

Change Summary Explanation

Fiscal Year (FY) 2017 includes a Congressional Add of $4.000 million for cyber vulnerabilities. FY 2019 difference between Previous President's Budget and Current President's Budget reflects a realignment of civilian pay to the Operations and Maintenance, Army (OMA) appropriation. The FY 2019 funding request was also reduced by $1.612 million to account for the availability of prior year execution balances.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army			Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	28.883	22.862	12.835	-	12.835	15.284	15.544	16.014	16.403	0.000	127.825
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 training and developmental and operational tests. 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 (PEO) required user testing in System Integration Laboratories and hardware/simulation in-the-loop facilities.

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 and tri-service capabilities to eliminate duplication of effort. These battlefield simulators represent systems (e.g. missile systems, command, control and communications systems, electronic warfare systems, etc.) that are used to portray a realistic threat environment during testing of U.S. weapon systems. Simulator development is responsive to Office of the Secretary of Defense and General Accounting 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 Instrumentation, Targets and Threat Simulators (PM ITTS) and the Director, Operational Test and Evaluation, Threat Simulator Investment Working Group.

Beginning in Fiscal Year (FY) 2019, this Project will also support the Advanced Electronic Support Sensor Suite (AESSS) and Cyber Blue Teams activities.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Title: Network Exploitation Test Tool (NETT).	3.683	3.675	1.552
Description: Engineering, Manufacturing and Development (EMD) for the NETT as a comprehensive Threat Cyberspace Operations (TCO) tool. Integrates new tools, tactics, and techniques into NETT to portray evolving Threat environments. NETT is a comprehensive TCO tool designed for Test and Evaluation (T&E) to portray evolving hostile and malicious Threat effects within the Cyber domain. Program will continue to provide an integrated suite of open-source/open-method exploitation tools to be integrated with robust reporting and instrumentation capabilities. NETT is used by TCO teams to replicate the tactics of state and non-state Threats and is supported by a robust TCO development environment. The Cyber domain will be the most rapidly changing domain in which our systems operate. NETT program will continue research of these capabilities and will use an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that will be needed during T&E. Focus			

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
areas include: continued Threat integration, instrumentation, distributed collaboration between multiple users, targets and attack visualization, data collection and remote agent development. ***FY 2018 Plans:*** Continues EMD phase for the NETT. Integrates new tools, tactics, and techniques into NETT to portray evolving Threat environments. Will continue research of these capabilities and will use an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that will be needed during T&E. Focus areas include: continued Threat integration, instrumentation, distributed collaboration between multiple users, targets and attack visualization, data collection and remote agent development. ***FY 2019 Plans:*** Continue EMD phase for the NETT including the integration of new tools, tactics, and techniques into the NETT to portray evolving Threat environments. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Realignment of civilian pay to the O&M, Army appropriation in FY19. Realignment of funds to higher Army priorities.			
Title: Threat Systems Management Office's (TSMO) Threat Operations ***Description:*** 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 test events including Network Evaluation Integration / Army Warfighting Assessment (NEI / AWA) and anticipated excursion test events for numerous Systems Under Test / Programs of Record (SUT / POR). ***FY 2018 Plans:*** Will continue to support multiple Army test events including NIE / AWA and anticipated excursion test events for numerous SUT / POR currently identified through FY18. ***FY 2019 Plans:*** Will continue to support multiple Army test events including NIE / AWA and anticipated excursion test events for numerous SUT / POR currently identified through FY19. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Realignment of civilian pay to the O&M appropriation in FY19.	3.395	3.627	1.357
Title: Integrated Threat Force (ITF), formerly named Threat Battle Command Center	1.965	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
Description: EMD phase for the ITF program to complete hardware / software development and Threat systems integration in support of the build-out of the threat force architecture. Full Operational Capability achieved in September 2017.			
Title: Threat Cyberspace Operations (TCO), formerly named Threat Computer Network Operations Team (TCNOT) ***Description:*** TCO supports ATEC events by maintaining a team of highly qualified, trained, and certified CNO professionals who execute Cyber operations against systems under test. The TCO program was designated a "Threat CNO Team" under Army Regulation (AR) 380-53 and is accredited as a United States Cyber Command (USCYBERCOM) / National Security Agency (NSA) certified "Red Team". ***FY 2018 Plans:*** Funding will support unique training, credentials, and authorizations for organizations such as Army Intelligence and Security Command (INSCOM), Deputy Chief of Staff (DCS) G2, NSA, and industry. FY18 plans include: continued research of intelligence-based TCO Tactics, Techniques, and Procedures (TTP) and Threat portrayal capabilities up to the Nation State level; development of a highly specialized TCO Training program; development, research, and analysis of continually emerging foreign threat capabilities; and data collection capability. ***FY 2019 Plans:*** Funding provides for Contractor subject matter expertise within the Cyber Red Team workforce to support critical threat assessments. Beginning in FY19, O&M funds will enable Cyber Red Team Department of the Army Civilian (DAC) subject matter expertise to execute this unique threat intelligence based mission. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Realignment of civilian pay to the O&M appropriation in FY19. Realignment of funds to higher Army priorities.	4.051	5.764	0.565
Title: Threat Cyberspace Operations (TCO) Fidelity Enhancements. formerly named Threat Computer Network Operations (CNO) Fidelity Enhancements ***Description:*** Establishes high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of TCO using commercial Information Technologies (IT) intended to engage complex U.S. operations. Threat packages range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt Army C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) and Enterprise Business Systems. ***FY 2018 Plans:***	1.333	1.402	0.762

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
Program will continue in FY18 to validate high-fidelity Threat malware and real-world tools, tactics, techniques, and procedures of Threat employment of CNO using commercial IT technologies intended to engage complex U.S. operations. Will continue to 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 range from "technological nomads" operating autonomously to state level forces using both active and passive network attack to selectively degrade or disrupt Army C4ISR and Enterprise Business Systems. ***FY 2019 Plans:*** Program will continue the validation of high-fidelity threat malware and real-world tools, tactics, techniques, and procedures of threat TCO employment using commercial IT technologies intended to engage complex U.S. operations. Will continue to 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 Army C4ISR and Enterprise Business Systems. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Realignment of civilian pay to the O&M appropriation in FY19.			
Title: Advanced Networked Electronic Support Threat Sensors (NESTS) ***Description:*** Program will begin prototype design and implementation to deliver advanced threat Electronic Support (ES) platforms. The Advanced NESTS program aims to increase existing Threat ES capabilities to match U.S. Intelligence Community performance assessments of real-world Threat capabilities. ***FY 2018 Plans:*** The Advanced NESTS program will continue to increase existing threat ES capabilities to match U.S. Intelligence Community performance assessments of real-world threat capabilities. This program seeks to replicate emerging real-world threat capabilities targeting advanced U.S. communication systems operating up to 18GHz. Program will continue the detailed design and the integration effort in pursuit of FOC during FY18. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** System achieves FOC in FY18. Beginning in FY19, this Program will transition to Advanced Electronic Support Sensor Suite (AESSS).	4.109	2.500	-
Title: Advanced Jammer Suite (AJS) ***Description:*** The Advanced Jammer Suite will continue to expand the Army's open air and alternatives for Electronic Attack (EA) in a test environment by using variations of jamming to include direct jamming, open air jamming and GPS jamming. It will keep the current jamming Threat as an asset to the Army for use in testing at lower test costs while expanding the Army alternative EA	4.394	3.000	2.079

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
in a test environment by using appropriate jamming techniques for the applied testing environment. This program continues Threat representation for the Army in the jamming domain, developing new and future jamming threats, to include satellite jamming. ***FY 2018 Plans:*** Threat development will include, but is not limited to, techniques such as Frequency Follower Direct Sequence Spread Spectrum (DSSS) threat jamming; Digital Radio Frequency Memory (DRFM) "spoofing," and extended Radio Frequency (RF) range into the Extremely High Frequency (EHF) range. ***FY 2019 Plans:*** Threat development will include, but is not limited to, techniques such as Frequency Follower Direct Sequence Spread Spectrum (DSSS) threat jamming; Digital Radio Frequency Memory (DRFM) "spoofing," and extended Radio Frequency (RF) range into the Extremely High Frequency (EHF) range. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Realignment of civilian pay to the O&M appropriation in FY19.			
Title: Threat Battle Command Force (TBCF), formerly named Integrated Threat Force (ITF) ***Description:*** The Threat Battle Command Force (TBCF) incorporates remote operations via distributed Command and Control (C2) while maintaining valid Threat TTP during T&E and training events. ***FY 2018 Plans:*** Integrate the Advanced NESTS system. Continue development of distributed C2 capabilities to support remote test operations. Will incorporate emerging Threat capabilities identified by the Intelligence Community. ***FY 2019 Plans:*** Integrate the Advanced Jammer Suite and additional Threat systems as identified by Threat assessments. Develop parsing tools to increase situational awareness for the Threat operations commander. Increase remote operations capabilities to decrease test costs. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Integration of different threat systems based upon Threat assessments.	1.953	2.237	2.370
Title: Next Generation Mobile Communication Network Infrastructure Test Range (Next GEN MCNITR) ***Description:*** Next Generation MCNITR provides a mobile, scalable closed-loop cellular communications network infrastructure implementing multiple technologies capable of providing a realistic commercial Radio Frequency (RF) signals environment needed for testing and training of U.S. forces in urban and suburban battle space environments. The Next Generation MCNITR	-	0.657	1.266

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
program acquires a capability that simulates real-world RF signals environment and that supports representative Threat force reliance of network enabled devices dependent on advanced cellular technology. ***FY 2018 Plans:*** Conduct risk reduction phase to decompose Threat requirements and system and sub-system functional requirements. Determine most efficient technology insertion schedule. ***FY 2019 Plans:*** Integrate commercial RF technologies to create a threat faithful communications environment based upon results of the risk reduction phase. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** FY18 transition from MCNITR to Next GEN MCNITR			
Title: Advanced Electronic Support Sensor Suite (AESSS) ***Description:*** AESSS provides expansion of Army's ability to portray acoustic, seismic, and electro-optical / infrared (EO/IR) sensor capabilities. ***FY 2019 Plans:*** Conduct risk reduction phase to decompose Threat requirements into system and sub-system functional requirements. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Beginning in FY19, this Program will transition from Advanced Networked Electronic Support Threat Sensors (NESTS).	-	-	1.959
Title: Management and oversight of Cyber Blue Team vulnerability assessments ***Description:*** In 2016 the Army Acquisition Executive (AAE) designated PM ITTS as the Office of Primary Responsibility for Acquisition Blue Teams, to provide management and execution of relevant Cyber Blue Team assessment capabilities in support of the acquisition and test communities. Cyber Blue Teams refer to the cyber team which works cooperatively with the system owner to ensure programs can defend against attackers and/or Red Teams. These Cyber Blue Team capabilities are essential to enable military operators to assess and defeat the presence of cyber security threats across Army networks. PM ITTS will also serve as the primary point of contact for cyber-related testing and vulnerabilities assessments with U.S. Cyber Command and Army Cyber. This Project executes the establishment and management of certification standards for Acquisition Blue Teams and coordination of Blue Team requirements on behalf of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA ALT). ***FY 2019 Plans:***	-	-	0.925

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
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 2017	FY 2018	FY 2019
This activity will establish and manage certification standards for Cyber Blue Teams in coordination with all Project Managers on behalf of Assistant Secretary of the Army for Acquisition, Logistics, and Technology. It will be the single point of contact with United States Cyber Command (CYBERCOM) for open and closed networks, and will develop and field a central repository for vulnerability assessments. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Cyber Blue Team Activities begin in FY19 for this Program.			
Accomplishments/Planned Programs Subtotals	24.883	22.862	12.835

	FY 2017	FY 2018
Congressional Add: Congressional Add - Cyber Vulnerabilities	4.000	-
FY 2017 Accomplishments: N/A		
Congressional Adds Subtotals	4.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

N/A