Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Army											Date: March 2014	
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 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
Total Program Element	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-
976: *Army Threat Sim (ATS)*	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-

The FY 2015 OCO Request will be submitted at a later date.

Note

FY13 adjustments attributed to Congressional General Reductions (-37 thousand); SBIR/STTR transfers (-244 thousand); and Sequestration reductions (-1.4 million).

A. Mission Description and Budget Item Justification

This program 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. 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 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 program 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 products and services, while providing the proper mix of resources needed to support Army testing and training. 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Army					Date: March 2014
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*			
B. Program Change Summary ($ in Millions)	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO**	**FY 2015 Total**
Previous President's Budget	18.090	16.934	19.180	-	19.180
Current President's Budget	16.409	23.921	18.062	-	18.062
Total Adjustments	-1.681	6.987	-1.118	-	-1.118
• Congressional General Reductions	-0.037	-0.013			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	7.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.244	-			
• Adjustments to Budget Years	-	-	-1.118	-	-1.118
• Other Adjustments	-1.400	-	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
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 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
976: *Army Threat Sim (ATS)*	-	16.409	23.921	18.062	-	18.062	18.780	22.599	20.403	21.352	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

Note

Threat Computer Network Operations (CNO) Fidelity Enhancements is a new start in FY15.

A. Mission Description and Budget Item Justification

This program supports the design, development, acquisition, integration, and fielding of realistic mobile threat simulators and realistic threat simulation products used in Army training, developmental tests, and operational tests. Project originally funded simulators representing Soviet equipment, but scope was expanded to address emerging world threats. Army Threat Simulator and Threat Simulation products are used to populate test battlefields for 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 program 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 products and services, while providing the proper mix of resources needed to support Army testing and training. 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 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, Threat Simulator Investment Working Group.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Network Exploitation Test Tool (NETT).	3.461	10.580	3.781
Articles:	-	-	-
Description: Continues Engineering Manufacturing and Development (EMD) for the NETT as a comprehensive Computer Network Operations (CNO) tool.			
FY 2013 Accomplishments: NETT is a comprehensive Computer Network Operations (CNO) tool, designed for T&E, to portray evolving hostile and malicious Threat effects within the cyber domain. The program provided an integrated suite of open-source/open-method exploitation tools which are integrated with robust reporting and instrumentation capabilities. NETT is used by Threat CNO teams to replicate the			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
tactics of state and non-state Threat and is supported by a robust CNO development environment. Current hacking tools and capabilities are introduced daily to hacking community. The NETT program researched these new capabilities and utilized an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that are needed during T&E. FY13 funding supported the continuation of exploit development, continues support to the NETT Users Group, and maintained pace with advanced exploit research and tool integration required to support the growing demand for the Threat CNO Team and mission. ***FY 2014 Plans:*** Continues EMD for the Network Exploitation Test Tool (NETT). NETT is a comprehensive Computer Network Operations (CNO) tool, designed for T&E, to portray evolving hostile and malicious Threat effects within the cyber domain. The program provides an integrated suite of open-source/open-method exploitation tools which will be integrated with robust reporting and instrumentation capabilities. NETT is used by Threat CNO teams to replicate the tactics of state and non-state Threat and is supported by a robust CNO development environment. The Cyber domain is the most rapidly changing domain in which our systems operate. The NETT program researches these new capabilities and uses 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, and remote agent development. ***FY 2015 Plans:*** Will continue EMD for the Network Exploitation Test Tool (NETT). NETT will be a comprehensive Computer Network Operations (CNO) tool, designed for T&E, to portray evolving hostile and malicious Threat effects within the cyber domain. The program will provide an integrated suite of open-source/open-method exploitation tools which will be integrated with robust reporting and instrumentation capabilities. NETT will be used by Threat CNO teams to replicate the tactics of state and non-state Threat and will be supported by a robust CNO development environment. The Cyber domain will be the most rapidly changing domain in which our systems operate. The NETT program will research these new 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 will include continued Threat integration, instrumentation, distributed collaboration, and remote agent development.			
Title: TSMO Threat Operations	2.704	2.868	2.838
Articles:	-	-	-
Description: Threat Systems Management Office's (TSMO) Threat Operations program manages, maintains, and sustains a mission ready suite of threat systems within the Army's Threat inventory. ***FY 2013 Accomplishments:*** Government Program Management for the TSMO Operations funded 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. Included acquisition life cycle management support (operation, maintenance, spares, new equipment training,			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
special tools and instrumentation, safety, environmental, security, information assurance, etc) of new threat systems fielded into the Army's Threat inventory. Funding supported the scheduled Life Cycle of equipment within the Threat inventory. ***FY 2014 Plans:*** Continuing the Threat Operations program funds 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 Integration Evaluation - NIE/Capabilities Integration Evaluation - CIE) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) currently identified through FY16. FY14 funding provides for acquisition life cycle management support and operation, maintenance, spares, new equipment training, special tools and instrumentation, additional DIACAP updates, etc, of new threat systems fielded into the Army's Threat inventory. ***FY 2015 Plans:*** Continuing 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 Integration Evaluation - NIE/Capabilities Integration Evaluation - CIE) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) currently identified through FY16. FY15 funding will provide for acquisition life cycle management support and operation, maintenance, spares, new equipment training, special tools and instrumentation, additional DIACAP updates, etc, of new threat systems fielded into the Army's Threat inventory.			
Title: Threat Intelligence and Electronic Warfare Environment (TIEW ENV).	2.286	3.813	3.736
Articles:	-	-	-
Description: Continues EMD for the Threat Intelligence and Electronic Warfare Environment (TIEW ENV) to simulate Electronic Warfare capabilities. ***FY 2013 Accomplishments:*** Continued EMD for the TIEW ENV: The TIEW ENV supports the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the EW capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV provides the capability to import vignettes, establishes virtual entities, connects live assets, and interacts between the live, virtual, and constructive environments. The TIEW ENV fully integrates with ITF to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY13 satisfied Army requirements by funding development, platform integration and sustainment of this capability. Program fields incremental capabilities in support of upcoming spin out events. ***FY 2014 Plans:***			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Continues EMD for the TIEW ENV: The TIEW ENV supports the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the Electronic Warfare (EW) capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV provides the capability to import vignettes, will establish virtual entities, connect live assets, and interact between the live, virtual, and constructive environments. The TIEW ENV fully integrates with the ITF to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY14 satisfies Army requirements by funding development, platform integration and sustainment of this capability. Program fields incremental capabilities in support of upcoming spin out events. Additional capabilities include the initial development of Threat Directed Energy Weapons (TDEW) model (which include threat Radio Frequency (RF) weapon simulators and instrumentation that employs next generation RF weapon capabilities against US Army systems that rely on survivable and robust sensors for C4ISR, continuous situational awareness, alert warning information and targeting) and continued integration with the ITF for robust LVC domain capability. The TIEW ENV also begins the integration, via the ITF, with the live Directed Energy Weapon assets and the Threat Unmanned Device. Integration with the Network Exploitation Test Tool (NETT) also begins in the latter part of FY14. ***FY 2015 Plans:*** Will continue EMD for the TIEW ENV: The TIEW ENV will support the establishment of a wrap-around threat environment required to evaluate, demonstrate, and employ the Electronic Warfare (EW) capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV will provide the capability to import vignettes, establish virtual entities, connect live assets, and interact between the live, virtual, and constructive environments. The TIEW ENV will fully integrate with the Intergrated Threat Force (ITF) to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY15 will satisfy Army requirements by funding development, platform integration and sustainment of this capability. Program will field incremental capabilities in support of upcoming spin out events. Will continue development of Threat Directed Energy Weapons (TDEW) models as well as Intelligence, Surveillance, and Reconnaissance (ISR) & Camouflage, Concealment, Deception and Obscurants (CCD&O) models. In addition, the TIEW ENV will continue integration, via ITF, with the live Directed Energy Weapon assets, the Threat Unmanned Device and the Network Exploitation Test Tool (NETT).			
Title: Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC)	4.510	3.916	3.481
Articles:	-	-	-
Description: Continues the EMD phase for the ITF program to continue hardware/software development and threat systems integration in support to the build-out of the threat force architecture. ***FY 2013 Accomplishments:*** Continued EMD for the ITF which provides an integrated, scalable Threat Command and Control for all Army Threat representations. This program leveraged prior Central Test & Evaluation Investment Program (CEIP) investments to create a highly adaptable and unique threat force capability to meet T&E requirements for the evaluation of network-centric platform and SoS capabilities by closely simulating expected real-world threat environments. FY13 funding was used for the continued			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
hardware/software development/build-out supporting the threat force architecture, visualization, Command and Control (C2), and fusion needs required to successfully meet salability and reconfigurability needs for current T&E requirements. ***FY 2014 Plans:*** Completes the EMD phase for Increment 3 of the ITF program to enhance the ITF's Threat Battle Command applications, the C3 interfaces with the Increment 1 and 2 threat systems as well as complete the integration of the Camouflage, Concealment, Deception, and Obscurants (CCD&O) assets. FY14 also delivers the final instrumentation capability for the ITF as well as completes the integration of the C2 functionality into the TBCC. FY14 funding is used to fulfill the Key Performance Parameters (KPPs) for Increment 3 while ensuring that the ITF program will continue to meet the C3 and data fusion needs required to successfully meet scalability and reconfigurability needs for current Test & Evaluation (T&E) requirements. ***FY 2015 Plans:*** Will initiate the EMD phase for Increment 4 of the ITF program to enhance the ITF's Threat Battle Command applications, the C3 interfaces with the Increment 1 - 3 threat systems as well as enhance the C2 functionality of the Threat Battle Command Center (TBCC). FY15 will support the initial design and development of distributed C2 functionality from the TBCC. will be used to fulfill the Key Performance Parameters (KPPs) for Increment 4 while ensuring that the ITF program will continue to meet the C3 and data fusion needs required to successfully meet scalability and reconfigureability needs for current T&E requirements.			
Title: Threat Computer Network Operations Teams (TCNOT)	3.448	2.744	2.946
Articles:	-	-	-
Description: The TCNOT supports Army Test and Evaluation events by maintaining a team of highly qualified, trained, and certified Computer Network Operations (CNO) professionals who execute cyber operations against systems under test. The TCNOT program was designated a "Threat CNO Team" under AR 380-53 recognized as a USSTRATCOM/NSA certified "Red Team". ***FY 2013 Accomplishments:*** Continued the Threat CNO Team program in establishing and maintaining a team of highly trained and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The Threat CNO Team mission is to accurately replicate the capabilities and hacker intent of state and non-state Threats through identification of Army system vulnerabilities that could be exploited by Threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. The funding supported unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. The FY13 funded requirements to include continued research of the intelligence-based TCNO Techniques, Tactics and Procedures (TTP) and threat portrayal capabilities up to the Nation State level; development of the necessary, highly specialized TCNO Training program; development, research, and analysis of continually emerging foreign threat capabilities; and data collection capability. The program established analytical services needed to identify			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
and correlate data of historical and real time malicious activity within the Army Land Warrior Network (LWN) and external to the DoD. This program also established services and near real-time processing of information needed to develop threat targeting packages that accurately profile the cyber enemy, types of systems they attack, frequency of attacks, their intent, doctrine, training, techniques, tools and operational tactics. The program resulted in creation of teams of Threat CNO professionals, working in concert with the Intelligence Community, capable of accurately portraying validated real world CNO threat to meet operational test requirements. ***FY 2014 Plans:*** Continues the Threat CNO Team program in establishing and maintaining a team of highly trained and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The Threat CNO Team mission is to accurately replicate the capabilities and hacker intent of state and non-state threats through identification of Army system vulnerabilities that could be exploited by threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. The funding supports unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. Funds requirements to include continued research of the intelligence-based TCNO Techniques, Tactics and Procedures (TTP) and threat portrayal capabilities up to the Nation State level; development of the necessary, highly specialized TCNO Training program; development, research, and analysis of continually emerging foreign threat capabilities; and data collection capability. ***FY 2015 Plans:*** Will continue the Threat CNO Team program in establishing and maintaining a team of highly trained and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The Threat CNO Team mission will be to accurately replicate the capabilities and hacker intent of state and non-state threats through identification of Army system vulnerabilities that could be exploited by threat forces, replicating loss of service, or exploiting network enabled systems to gain critical information or create a desired effect. The funding will support unique training, credentials, and authorizations involving organizations such as Army 1st IO Command, NSA, HQDA-G2, and industry. The FY15 will fund requirements to include continued research of the intelligence-based TCNO Techniques, Tactics and Procedures (TTP) and threat portrayal capabilities up to the Nation State level; development of the necessary, highly specialized TCNO Training program; development, research, and analysis of continually emerging foreign threat capabilities; and data collection capability.			
Title: Threat Computer Network Operations (CNO) Fidelity Enhancements	-	-	1.280
Description: Threat CNO Fidelity Enhancements is a new start project that will establish 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.			
FY 2015 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
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, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Program will establish validated 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. This program 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 that will not be available to evaluate the exploitation of existing vulnerabilities in Enterprise Business Systems and network enabled systems. 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.			
Accomplishments/Planned Programs Subtotals	16.409	23.921	18.062

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

THREAT SIMULATOR Test Programs Supported: Aircraft (MH-47E) Follow On Operational Test II, MH-60K Aircraft, Aircraft (MH-60K) Follow On Operational Test II, RAH-66 Comanche EUTE, RAH-66 Comanche FDTE I, Suite of Integrated Radio Countermeasures (SIRFCM), Suite of Integrated Radio Countermeasures (SIIRCM), Unmanned Aerial Vehicle (UAV) - Payload, Force XXI Battle Command Brigade and Below, Army Airborne Command and Control, Army TACMS Block II/BAT, Bradley Fighting Vehicle-A3, Crusader FDTE, Extended Range MLRS, FAAD Block III, GPS in Joint Battle Space Environment, Guardrail/Common Sensor System II, Handheld Standoff Mine Field Detection System, IEW Tactical Proficiency Trainer, Joint Close Air Support HT&E, Joint Suppression of Enemy Air Defense (JSEAD), Land Warrior, Long Range Advanced Scout Surveillance System, Navigational Warfare Global Positioning System, OH-58D Kiowa Warrior, Patriot Advanced Capabilities PAC-3 Config-3, UH-60Q, Theater High Altitude Area Defense System.

E. Performance Metrics

N/A