Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Army											DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*					R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*							
COST ($ in Millions)	**All Prior Years**	**FY 2012**	**FY 2013#**	**FY 2014 Base**	**FY 2014 OCO ##**	**FY 2014 Total**	**FY 2015**	**FY 2016**	**FY 2017**	**FY 2018**	**Cost To Complete**	**Total Cost**
Total Program Element	-	25.838	18.090	16.934	-	16.934	19.180	22.863	22.932	20.697	Continuing	Continuing
976: *ARMY THREAT SIM (ATS)*	-	25.838	18.090	16.934	-	16.934	19.180	22.863	22.932	20.697	Continuing	Continuing

FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

The FY 2014 OCO Request will be submitted at a later date

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. While this project originally funded simulators representing Soviet equipment, the changing world order has expanded the scope of this program to address other 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.

B. Program Change Summary ($ in Millions)	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total
Previous President's Budget	26.117	18.090	16.934	-	16.934
Current President's Budget	25.838	18.090	16.934	-	16.934
Total Adjustments	-0.279	0.000	0.000	-	0.000
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.279	-			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army			DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*	

COST ($ in Millions)	All Prior Years	FY 2012	FY 2013#	FY 2014 Base	FY 2014 OCO ##	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
976: *ARMY THREAT SIM (ATS)*	-	25.838	18.090	16.934	-	16.934	19.180	22.863	22.932	20.697	Continuing	Continuing
Quantity of RDT&E Articles												

FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

The FY 2014 OCO Request will be submitted at a later date

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. While this project originally funded simulators representing Soviet equipment, the operational environment has expanded the scope of this program to address other 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 2012	FY 2013	FY 2014
Title: Network Exploitation Test Tool (NETT).	3.287	3.461	3.580
Articles:	0	0	
Description: Continues Engineering Manufacturing and Development (EMD) for the NETT as a comprehensive Computer Network Operations (CNO) tool.			
FY 2012 Accomplishments: Continued EMD for the Network Exploitation Test Tool (NETT). Network Exploitation Test Tool 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 were integrated with robust reporting and instrumentation capabilities. NETT was used by Threat CNO teams to replicate the tactics of state and non-state Threat and was supported by a robust CNO development environment. Current hacking tools and capabilities were			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
being introduced daily to the hacking community. The NETT program researched these new capabilities and used an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that were needed during T&E. Funding in FY12 allowed for the continued integration of these threats and tools, including an Application Programming Interface (API). Updated Information Assurance and Threat validation certifications required for T&E were also supported. ***FY 2013 Plans:*** 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 are 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. Current hacking tools and capabilities are introduced daily to hacking community. The NETT program researches these new capabilities and utilizes an in-depth process to clean, fix, and integrate required Threat tools, tactics, and techniques that are needed during T&E. FY13 funding supports the continuation of exploit development, continues support to the NETT Users Group, and will maintain pace with advanced exploit research and tool integration required to support the growing demand for the Threat CNO Team and mission. ***FY 2014 Plans:*** Will continue EMD for the Network Exploitation Test Tool (NETTS). 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 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: Congressional Add - Threat Simulator Development Unfunded Joint Forces Command (JFCOM) Mission Transfer. ***Articles:*** ***Description:*** Completes the engineering and manufacturing Development (EMD) for Joint Forces Command (JFCOM) Mission Transfer. ***FY 2012 Accomplishments:*** Completed the Engineering and Manufacturing Development (EMD) required to facilitate the seamless Joint Forces Command (JFCOM) Mission Transfer.	9.043 0	0.000	0.000
Title: TSMO Threat Operations	2.904	2.704	2.868

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
Articles:	0	0	
Description: Threat Systems Management Office's (TSMO) Threat Operations program manages, maintains, and sustains a mission ready suite of of threat systems within the Army's Threat inventory. ***FY 2012 Accomplishments:*** The Threat Operations program satisfied the requirement to provide operational support and mission ready sustainment of threat systems that included maintenance, spares, special tools, threat TTP training, recurring DIACAP updates, entry and drawdown of threat assets, storage and sustainment facilities associated with fielded Threat systems and infrastructure. The Threat Operations program had successfully supported two major (Network Integration Evaluation - NIE) and multiple excursion Army test events for numerous Systems Under Test (SUT)/Programs of Record (POR) including Joint Tactical Radio System (JTRS) Handheld, Manpack, and Small Form Fit (HMS), Rifleman Radio, Warfighter Information Network-Tactical (WIN-T) with outstanding recognition for support. ***FY 2013 Plans:*** Government Program Management for the TSMO Operations 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. Includes acquisition life cycle management support (operation, maintenance, spares, new equipment training, special tools and instrumentation, safety, environmental, security, information assurance, etc) of new threat systems fielded into the Army's Threat inventory. Funding supports the scheduled entry and drawdown of equipment within the Threat inventory. ***FY 2014 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) and anticipated excursion test events for numerous Systems Under Test (SUT)/Programs of Record (POR) not currently identified but anticipated (TBD). FY14 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).	3.973	3.967	3.813
Articles:	0	0	
Description: Continues EMD for the Threat Intelligence and Electronic Warfare Environment (TIEW ENV) to simulate Electronic Warfare capabilities. ***FY 2012 Accomplishments:***			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
Continued EMD for the TIEW ENV: TIEW ENV provided the constructive Threat representation environment for Army T&E and provided the primary capability to interact between live, virtual, and constructive Threat Information Operations (IO) environments. The TIEW ENV integrated Threat IO (Electronic Attack, Electronic Support, Computer Network Operations) models into the One Semi-Automated Force (OneSAF) baseline. The models' representative effects were also integrated through use with Communications Effects Servers. Integration of OneSAF with the Integrated Threat Force (ITF) enabled the Live and Constructive T&E environments to interface. To date the program had completed numerous models to include Communications Jamming (simulates frequencies, ranges, spot, barrage, and other behaviors); Global Positioning Satellite (GPS) Jamming (can jam GPS frequencies in variety of ways by adjusting the parameters and can emulate real GPS jammers); GPS Repeater Jammer (offset GPS signals so as to provide false location reports. Had several adjustable behavioral parameters); Spoofer Jammer (offsets GPS signals so as to provide false location reports with several adjustable behavioral parameters); and Signal Intelligence/ Direction Finding (SIGINT/DF) (detector models that work with each other to triangulate and then report on emissions of various frequencies and was parameter adjustable). The program continued to develop the Computer Network Operations (CNO) cyber model which build CNO entities (hacker entities, systems, networks, etc.) that can be attacked, defended, and exploited (Disruption, Delay, Denial of Service, Destruction, and Injection) as well as allowed live attacks to interact with the constructive environment for large enterprise asset emulation cyber attacks, all within OneSAF. The program also began the development of the Threat Cellular Network Model (TCNM) which was building the threat cellular and landline interfaces needed to emulate the communications systems often found in theater as used by enemy combatants. The TIEW ENV program also integrated the capability to communicate, via the ITF, with live assets including the CICADA jammer, Threat Signal Injection Jammers (TSIJ), Wideband Configurable Controlled Jammer (WCCJ) and the Networked Electronic Support Threat Sensors (NESTS). ***FY 2013 Plans:*** 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 EW capabilities of Enemy Forces in simulated real-world test/training events. The TIEW ENV provides the capability to import vignettes, establishes virtual entities, conects 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 satisfies Army requirements by funding development, platform integration and sustaiment of this capability. Program fields incremental capabilities in support of upcoming spin out events. ***FY 2014 Plans:*** Will continues 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, will establish virtual entities, connect live assets, and interact between the live, virtual, and constructive environments. The TIEW ENV will fully integrate with the ITF to enable Opposing Forces (OPFOR) command of threat EW assets across Live, Virtual, and Constructive (LVC) domains. FY14			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
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. Additional capabilities will include the initial development of Threat Directed Energy Weapons (TDEW) model (which will include threat Radio Frequency (RF) weapon simulators and instrumentation that will employ 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 will also begin 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) will also begin in the latter part of FY14.			
Title: Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC)	3.847	4.510	3.916
Articles:	0	0	
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 2012 Accomplishments: The ITF Program completed Engineering and Manufacturing Development (EMD) phase for Increment 2 of the ITF program. The activities completed during this effort included enhancement to the ITF's threat battle command applications to provide increased capability in the areas of Command and Control (C2), Situational Awareness (SA) Visualization, Collaboration and Communications. The ITF also enhanced its Command, Control and Communications (C3) interfaces with the Increment 1 threat systems (TSIJ, NETT, NESTS, and TIEW ENV) while also performing the integration of the Mobile Commercial Network Infrastructure Test Range (MCNITR), Threat Unmanned Devices (TUD), Wideband Configurable Controllable Jammer (WCCJ), and CICADA. The completion of the EMD phase for Increment 2 provided an integrated, scalable Threat command and control for all Army Threat representations to provide the T&E solution to satisfy the SoS requirement of a Free Thinking Threat force.			
FY 2013 Plans: Continues EMD for the ITF which provides an integrated, scalable Threat command and control for all Army Threat representations. This program leverages 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 is used for the continued hardware/ software development/build-out supporting the threat force architecture, visualization, Command and Control (C2), and fusion needs required to successfullly meet salability and reconfigurability needs for current T&E requirements.			
FY 2014 Plans: Will complete the EMD phase for Increment 3 of the ITF program to enhance the ITF's threat battle command applications, enhance the C3 interfaces with the Increment 1 and 2 threat systems as well as complete the integration of the CCD&O assets.			

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
FY14 will also deliver the final instrumentation capability for the ITF as well as complete the integration of the C2 functionality into the TBCC. FY14 will also provide for the procurement of the initial spares to support the Increment 3 hardware and software baselines. FY14 funding will be 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 T&E requirements.			
Title: Threat Signal Injection Jammer (TSIJ), a suite of threat electronic Attack (EA) assets in suppport of operational test events and training exercises. ***Articles:*** ***Description:*** Continues the Engineering Manufacturing Development (EMD) for the TSIJ program to provide the Army with Electronic Attack in an open air environment along with alternatives to open-air Electronic Attack (EA) in a test and training support role. ***FY 2012 Accomplishments:*** Completed EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input of threat jamming waveforms into a receiver unit and remote control on/off employment. Developed design for 2-channel man-pack Remote Jamming Unit (RJU) installed in a soldier's "bullit-proof" vest (Improved Outer Tactical Vest - IOTV) and employing its own power source) all without added weight to the vest and 10 watt environmentally sealed Control Signal Transmitter (CST) for unmanned operations in remote locations.	0.406 0	0.000	0.000
Title: Threat Computer Network Operations Teams (TCNOT) ***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. ***FY 2012 Accomplishments:*** Continued EMD for the Threat CNO Team program. Threat CNO Team program established and maintained 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 was to accurately replicate the hacker intent of state and non-state Threats through identification of 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. During FY12, the TCNOT program was designated a "Threat CNO Team" under AR380-53, recognized as a USSTRATCOM/NSA certified "Red Team," and executed cyber test and evaluation against systems	2.378 0	3.448 0	2.757

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2012	FY 2013	FY 2014
including but not limited to: Defense Common Ground Station – Army (DCGS-A), Warfighter Information Network Tactical (WIN-T), Apache Block III, GRAY EAGLE, and Global Combat Supply System (GCSS). ***FY 2013 Plans:*** Continues EMD for the Threat CNO Team program. The Threat CNO Team program establishes and maintains 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. The FY13 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. The program establishes analytical services needed to identify 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 establishes 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 results in creation of teams of Threat CNO professional, working in concert with the Intelligence Community, capable of accurately protraying validated real world CNO threat to meet operational test requirements. ***FY 2014 Plans:*** Will continue EMD for the Threat CNO Team program. The Threat CNO Team program will establish and maintain 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 FY14 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. Systems Tested include: Kiowa Warrior, Mid-Tier Network Vehicle Radio, DCGS-A, AN/TPQ-53, Joint Tactical Radio System (JTRS), EMARSS.			
Accomplishments/Planned Programs Subtotals	25.838	18.090	16.934

Exhibit R-2A, RDT&E Project Justification: PB 2014 Army		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 2040: *Research, Development, Test & Evaluation, Army* BA 6: *RDT&E Management Support*	R-1 ITEM NOMENCLATURE PE 0604256A: *THREAT SIMULATOR DEVELOPMENT*	PROJECT 976: *ARMY THREAT SIM (ATS)*

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

Performance metrics used in the preparation of this justification material may be found in the FY 2010 Army Performance Budget Justification Book, dated May 2010.