

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Army **DATE:** February 2011

| | |
|--|--|
| APPROPRIATION/BUDGET ACTIVITY 2040: <i>Research, Development, Test & Evaluation, Army</i> BA 6: <i>RDT&E Management Support</i> | R-1 ITEM NOMENCLATURE PE 0604256A: <i>THREAT SIMULATOR DEVELOPMENT</i> |
|--|--|

| COST (\$ in Millions) | FY 2010 | FY 2011 | FY 2012 Base | FY 2012 OCO | FY 2012 Total | FY 2013 | FY 2014 | FY 2015 | FY 2016 | Cost To Complete | Total Cost |
|-----------------------------------|---------|---------|--------------|-------------|---------------|---------|---------|---------|---------|------------------|------------|
| Total Program Element | 23.120 | 26.158 | 16.992 | - | 16.992 | 17.442 | 17.213 | 17.014 | 17.229 | Continuing | Continuing |
| 976: <i>ARMY THREAT SIM (ATS)</i> | 23.120 | 26.158 | 16.992 | - | 16.992 | 17.442 | 17.213 | 17.014 | 17.229 | Continuing | Continuing |

Note

None Required.

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 2010 | FY 2011 | FY 2012 Base | FY 2012 OCO | FY 2012 Total |
|---|----------------|----------------|---------------------|--------------------|----------------------|
| Previous President's Budget | 25.091 | 26.158 | 17.300 | - | 17.300 |
| Current President's Budget | 23.120 | 26.158 | 16.992 | - | 16.992 |
| Total Adjustments | -1.971 | - | -0.308 | - | -0.308 |
| • Congressional General Reductions | | - | | | |
| • Congressional Directed Reductions | | - | | | |
| • Congressional Rescissions | - | - | | | |
| • Congressional Adds | | - | | | |
| • Congressional Directed Transfers | | - | | | |
| • Reprogrammings | -1.500 | - | | | |
| • SBIR/STTR Transfer | -0.471 | - | | | |
| • Adjustments to Budget Years | - | - | -0.308 | - | -0.308 |

UNCLASSIFIED

UNCLASSIFIED

| | | | | | | | | | | | |
|---|---------|---------|--------------|--|---------------|---------|---------|---------------------------------------|------------|------------------|------------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | | | | | | | DATE: February 2011 | | | |
| 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) | FY 2010 | FY 2011 | FY 2012 Base | FY 2012 OCO | FY 2012 Total | FY 2013 | FY 2014 | FY 2015 | FY 2016 | Cost To Complete | Total Cost |
| 976: ARMY THREAT SIM (ATS) | 23.120 | 26.158 | 16.992 | - | 16.992 | 17.442 | 17.213 | 17.014 | 17.229 | Continuing | Continuing |
| Quantity of RDT&E Articles | | | | | | | | | | | |
| A. Mission Description and Budget Item Justification | | | | | | | | | | | |
| <p>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.</p> | | | | | | | | | | | |
| B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each) | | | | | | | | FY 2010 | FY 2011 | FY 2012 | |
| <p>Title: Continues Engineering Manufacturing and Development (EMD) for the Network Exploitation Test Tool (NETT).</p> <p>Articles:</p> <p>Description: Continues EMD for the NETT as a comprehensive Computer Network Operations (CNO) tool.</p> <p>FY 2010 Accomplishments: Continues EMD for the Network Exploitation Test Tool (NETT) as a comprehensive Computer Network Operations (CNO) tool, designed for Test & Evaluation (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 and has steadily incorporated leading Threat tools, tactics, techniques, and procedures.</p> <p>FY 2011 Plans:</p> | | | | | | | | 3.558 0 | 3.253 0 | 3.332 | |

UNCLASSIFIED

UNCLASSIFIED

| | | | | | |
|---|--|--|--------------------------------|---|----------------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | | DATE: February 2011 | | |
| APPROPRIATION/BUDGET ACTIVITY 2040: <i>Research, Development, Test & Evaluation, Army</i> BA 6: <i>RDT&E Management Support</i> | | R-1 ITEM NOMENCLATURE PE 0604256A: <i>THREAT SIMULATOR DEVELOPMENT</i> | | PROJECT 976: <i>ARMY THREAT SIM (ATS)</i> | |
| B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each) | | | FY 2010 | FY 2011 | FY 2012 |
| Continues EMD for the Network Exploitation Test Tool (NETT) as a comprehensive Computer Network Operations (CNO) tool, designed for Test & Evaluation (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 and has steadily incorporated leading Threat tools, tactics, techniques, and procedures. | | | | | |
| FY 2012 Plans: Continues 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 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 being introduced daily to the hacking community. 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 are needed during T&E. | | | | | |
| Title: Government Program Management for the Threat Systems Management Office Operations (TSMO). Description: Government Program Management for TSMO. FY 2010 Accomplishments: The Government Program Management for the Threat Systems Management Office Operations funds the operation, maintenance management, and sustainment capability for Threat systems within the Army's Threat inventory. Satisfies the requirement to provide operations and maintenance, spares, training, special tools, recurring DIACAP, etc, for fielded Threat systems and infrastructure. Funding supports manpower, storage, and integration facilities associated with the sustainment and operational readiness of the Army's Threat force. FY 2011 Plans: The Government Program Management for the Threat Systems Management Office Operations funds the operation, maintenance management, and sustainment capability for Threat systems within the Army's Threat inventory. Satisfies the requirement to provide operations and maintenance, spares, training, special tools, recurring DIACAP, etc, for fielded Threat systems and infrastructure. Funding supports manpower, storage, and integration facilities associated with the sustainment and operational readiness of the Army's Threat force. FY 2012 Plans: | | | Articles: 1.968 0 | 1.851 0 | 2.895 |

UNCLASSIFIED

UNCLASSIFIED

| | | | | | | |
|---|--|--|---------------------|---------------------------------------|------------|---------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | | DATE: February 2011 | | | |
| 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 2010 | FY 2011 | FY 2012 |
| Government Program Management for the TSMO Operations funds the operation, maintenance management, and sustainment capability for Threat systems within the Army's Threat inventory. Funding supports manpower, storage, and integration facilities associated with the sustainment and operational readiness of the Army's Threat force. Satisfies the requirement to provide operations and maintenance, spares, training, special tools, recurring Department of Defense Information Assurance and Certification Process (DIACAP), etc, for fielded Threat systems and infrastructure. | | | | | | |
| Title: Continues Engineering and Manufacturing Development (EMD) for the Threat Intelligence and Electronic Warfare (IEW). Articles: Description: Continues EMD for the Threat Intelligence and Electronic Warfare (IEW) Environment to simulate Electronic Warfare capabilities. FY 2010 Accomplishments: Continues EMD for the Threat Intelligence and Electronic Warfare (IEW) Environment that provides the constructive Threat representation environment for Army T&E and provides the primary capability to interact between live, virtual, and constructive Threat Information Operations (IO) environments. FY 2011 Plans: Continues EMD for the Threat Intelligence and Electronic Warfare (IEW) Environment that provides the constructive Threat representation environment for Army T&E and provides the primary capability to interact between live, virtual, and constructive Threat Information Operations (IO) environments. FY 2012 Plans: Continues EMD for the Threat Intelligence Electronic Warfare Environment. Threat Intelligence Electronic Warfare Environment provides the constructive Threat representation environment for Army T&E and provides the primary capability to interact between live, virtual, and constructive Threat IO environments. The Threat IEW Environment integrates Threat IO (Electronic Attack, Electronic Support, CNO) models into the One Semi-Automated Force (OneSAF) baseline. The models' representative effects are also integrated through use with Communications Effects Servers. Integration of OneSAF with the Integrated Threat Force (ITF) enables the Live and Constructive T&E environments to interface. | | | | 3.035 0 | 3.874 0 | 4.039 |
| Title: Completes the Engineering and Manufacturing Development (EMD) for the Electronic Combat and Counter Terrorism Training Range. Articles: Description: Completes the EMD for the FY10 Electronic Combat and Counter Terrorism Training Range Congressional Add. FY 2010 Accomplishments: | | | | 2.928 0 | - | - |

UNCLASSIFIED

UNCLASSIFIED

| | | | | |
|--|--|---------------------------------------|------------|---------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | DATE: February 2011 | | |
| 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 2010 | FY 2011 | FY 2012 |
| Completes EMD for the FY10 Electronic Combat and Counter Terrorism Training Range Congressional Add. This was a follow-on to FY08-09 Congressional Adds for Townsend Electronic Training Range. | | | | |
| Title: Continues the Engineering and Manufacturing Development (EMD) for the Integrated Threat Force (ITF), formerly named Threat Battle Command Center (TBCC) to support new threat systems/equipment. Articles: Description: Continues the EMD for the ITF to support new threat systems/equipment. FY 2010 Accomplishments: Continues the EMD for the ITF that will provide an integrated, scalable Threat command and control for all Army Threat representations as well as provide the Test & Evaluation (T&E) solution to satisfy the SoS requirement of a Free Thinking Threat force. FY 2011 Plans: Continues the EMD for the ITF that will provide an integrated, scalable Threat command and control for all Army Threat representations as well as provide the Test & Evaluation (T&E) solution to satisfy the SoS requirement of a Free Thinking Threat force. FY 2012 Plans: Continues EMD for the ITF which provides an integrated, scalable Threat command and control for all Army Threat representations to provide the T&E solution to satisfy the System of Systems requirement of a Free Thinking Threat force. | | 3.292 0 | 3.858 0 | 3.908 |
| Title: Continues the Engineering and Manufacturing Development (EMD) for the Threat Signal Injection Jammer (TSIJ). Articles: Description: Continues the EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment. FY 2010 Accomplishments: Continues the EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input to a receiver unit and remote control on/off employment. FY 2011 Plans: Continues the EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input to a receiver unit and remote control on/off employment. FY 2012 Plans: | | 2.833 0 | 1.128 0 | 0.417 |

UNCLASSIFIED

UNCLASSIFIED

| | | | | | | |
|---|--|---|---------------------|---------------------------------------|------------|---------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | | DATE: February 2011 | | | |
| 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 2010 | FY 2011 | FY 2012 |
| Continues EMD for the TSIJ to provide the Army an alternative to open-air Electronic Attack (EA) in a test environment by using direct input to a receiver unit and remote control on/off employment. Develop design for 2-channel man-pack Remote Jamming Unit (RJU) and 10 watt environmentally sealed Control Signal Transmitter (CST) for TSIJ. | | | | | | |
| Title: Continues the Engineering and Manufacturing Development (EMD) for the Control of Signal Transmission-Open Air Capability (CST-OAC) and Signal Intelligence/Direct Finding (SIGINT/DF). Articles: Description: Continues the EMD for the CST-OAC and SIGINT/DF sensors onto a larger aerial platform for Threat Devices capability. FY 2010 Accomplishments: Continues the EMD for the CST-OAC and SIGINT/DF sensors onto a larger aerial platform for Threat Devices capability. FY 2011 Plans: Completes EMD for the CST-OAC and SIGINT/DF sensors onto a larger aerial platform for Threat Devices capability. | | | | 2.052 0 | 0.667 0 | - |
| Title: Completes the Engineering and Manufacturing Development (EMD) for the Networked Electronic Support Threat Sensors (NESTS). Articles: Description: Completes the EMD for the NESTS systems. FY 2010 Accomplishments: Completes the EMD for the NESTS systems. Developed NESTS systems up to 3GHz for integration within the Force. | | | | 1.644 0 | - | - |
| Title: Continues Government Program Management for the Threat Computer Network Operations Teams (TCNOT) to support threat events. Articles: Description: Continues Government Program Management for the TCNOT to support threat events in order to maintain a team of highly qualified, trained, and certified Computer Network Operations (CNO) professionals qualified for the employment of Threat CNO in support of Army T&E. FY 2010 Accomplishments: Continues Government Program Management for the Threat Computer Network Operations Teams (TCNOT) to support threat events in order to maintain a team of highly qualified, 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 hacker intent of state and non- | | | | 1.810 0 | 2.327 0 | 2.401 |

UNCLASSIFIED

UNCLASSIFIED

| | | | | | |
|---|--|--|----------------------------|---|----------------|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | | DATE: February 2011 | | |
| APPROPRIATION/BUDGET ACTIVITY 2040: <i>Research, Development, Test & Evaluation, Army</i> BA 6: <i>RDT&E Management Support</i> | | R-1 ITEM NOMENCLATURE PE 0604256A: <i>THREAT SIMULATOR DEVELOPMENT</i> | | PROJECT 976: <i>ARMY THREAT SIM (ATS)</i> | |
| B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each) | | | FY 2010 | FY 2011 | FY 2012 |
| 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. FY 2011 Plans: Continues Government Program Management for the Threat Computer Network Operations Teams (TCNOT) to support threat events in order to maintain a team of highly qualified, trained, and certified CNO professionals qualified for the employment of Threat CNO in support of Army T&E. The mission is for the Threat CNO Team 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. FY 2012 Plans: Continues EMD for the Threat CNO Team program. 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 "hacker" intent of state and non-state Threats through identification of system vulnerabilities that could b exploited by Threat forces, replicating loss of service or exploiting network enabled systems to gain critical information or create a desired effect. Funding supports unique training, credentials, and authorizations involving organizations such as the Army 1st Information Operations Command, National Security Agency, Army Office of the Deputy Chief of Staff - Intelligence (Army G-2), and industry. Army G-2 specifically granted exception to policy for TSMO to conduct open-network Threat CNO testing in support of Army T&E. | | | | | |
| Title: Army Technical Test Instrumentation and Targets Project 62C Modeling and Simulation Instrumentation Articles: Description: Project 976 includes \$9,200K FY11 RDTE incorrectly placed in this funding line. FY 2011 Plans: Project 976 includes \$9,200K FY11 RDTE incorrectly placed in this funding line. It was intended for 0605602A - Army Technical Test Instrumentation and Targets Project 62C Modeling and Simulation Instrumentation in support of operational and developmental testing. | | | - | 9.200 0 | - |
| Accomplishments/Planned Programs Subtotals | | | 23.120 | 26.158 | 16.992 |
| | | | | | |

UNCLASSIFIED

UNCLASSIFIED

| | | |
|--|--|---|
| Exhibit R-2A, RDT&E Project Justification: PB 2012 Army | | DATE: February 2011 |
| APPROPRIATION/BUDGET ACTIVITY 2040: <i>Research, Development, Test & Evaluation, Army</i> BA 6: <i>RDT&E Management Support</i> | R-1 ITEM NOMENCLATURE PE 0604256A: <i>THREAT SIMULATOR DEVELOPMENT</i> | PROJECT 976: <i>ARMY THREAT SIM (ATS)</i> |

C. Other Program Funding Summary (\$ in Millions)

N/A

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.

UNCLASSIFIED