Exhibit R-2, RDT&E Budget Item Justification: PB 2016 The Joint Staff	Date: February 2015
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0303166J *I Support to Information Operations Capability*

COST ($ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
Total Program Element	3.975	8.348	11.552	10.413	-	10.413	10.576	10.700	10.700	10.700	Continuing	Continuing
001: *Information Operations Range*	3.975	8.348	11.552	10.413	-	10.413	10.576	10.700	10.700	10.700	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Joint Information Operations Range (JIOR) provides DoD a closed-loop, persistent, geographically distributed network to conduct training, testing, and experimentation in support of Computer Network Attack (CNA)/Computer Network Defense (CND) in a threat representative environment with realistic and relevant targets and command & control systems of interest. JIOR uniquely provides Services, Combatant Commanders (CCMD), and other government agencies the ability to test deployment and collaboratively gain insights into advanced Cyberspace, Information Operations (IO), and Electronic Warfare (EW) capabilities under current and future operational environment conditions. JIOR integrates other cyberspace ranges, replicates critical infrastructure, cyber targets, Internet traffic, and opposing forces. These provide the capacity to meet Presidential policy and CJCS mandates for training and certification of 6000+ cyber warriors by 2017 and DoD/Interagency cyber vulnerability assessments. The JIOR security construct allows users to develop, test, and secure their unique cyber capabilities and protect their identity during range activities. The JIOR conducts multiple, simultaneous, and disparate training, testing, and experimentation events.

B. Program Change Summary ($ in Millions)	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total
Previous President's Budget	8.394	11.552	10.413	-	10.413
Current President's Budget	8.348	11.552	10.413	-	10.413
Total Adjustments	-0.046	-	-	-	-
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Carry-over from FY2014	-0.046	-	-	-	-

Change Summary Explanation

The increase in funding between FY2014 and FY2015 improves Joint IO range training & assessment throughput capacity to address CJCS mandates.
The change from FY15 to FY16 is $0.161 increase in funding baseline and a decrease in funding due to a zero-based transfer of $1.3M from RDT&E to O&M to properly align labor costs with operations.

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 The Joint Staff	Date: February 2015
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0303166J *I Support to Information Operations Capability*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2014	FY 2015	FY 2016
Title: Information Operations Range	8.348	11.552	10.413
Description: The Joint Information Operations Range (JIOR) is a closed-loop network that forms a live-fire range utilizing encrypted tunneling over existing networks to conduct training, testing, and experimentation in support of Information Operations (IO), Electronic Warfare (EW), Computer Network Attack (CNA)/Computer Network Defense (CND)), and Cyberspace mission areas in a threat representative environment. ***FY 2014 Accomplishments:*** (1) Increased JIOR capacity to support a 50 percent increase in user demand for training, testing, and experimentation event support through site expansion and development of new persistent environments. Increased JIOR capabilities, expanding Network Operations & Security Center (NOSC) coverage (12x5) to support increased user demand; completed proof-of-concept as precursor to transition to hybrid Defense Research and Engineering Network – Defense Information Systems Network (DREN-DISN) transport circuit solution. (2) Developed asd began fielding Live Laboratory Advanced Visual Analytics (LAVA); 1 Gigabits per second (Gbps) capable JIOR service delivery points. (3) Reduced risk by completion of deferred critical lifecycle maintenance& deployment of improved network test equipment. ***FY 2015 Plans:*** (1) Expand national DoD and Inter-Agency awareness and support regarding IO and cyber related activities (2) Improve the threat representation and operational relevance of the network (3) Improve the integration of Live Virtual Constructive (LVC) simulations with other Joint training and testing communities and infrastructures ***FY 2016 Plans:*** Continues FY2015 efforts: (1) Expand national DoD and Inter-Agency awareness and support regarding IO and cyber related activities (2) Improve the threat representation and operational relevance of the network (3) Improve the integration of LVC simulations with other Joint training and testing communities and infrastructures			
Accomplishments/Planned Programs Subtotals	8.348	11.552	10.413

D. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 The Joint Staff	Date: February 2015
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0303166J *I Support to Information Operations Capability*

E. Acquisition Strategy

The Joint IO Range manages the development and expansion of Joint IO Range capabilities to an increasing number of customers. Integration into the Joint Exercise program has allowed users to increase the use and capability of the range. Continued development of tools for the range will be required as adversarial capabilities improve. Automation of JIOR scheduling and network reconfiguration will be critical to increasing capacity and meeting user demands.

F. Performance Metrics

RDT&E development efforts are evaluated based on the performance metrics. This ensures the JIOR capacity and capability development funding is synchronized against prioritized training and testing requirements, based on designs derived and tested against synchronized requirements, and result in deployed capabilities that are within the enterprise's capacity to deliver. Performance metrics include, but are not limited to; cost, time, relevancy, and analytics and as defined below:

• Cost – Does the effort enable the most cost effective cyber training?
• Time – Will the effort enable trainers/ testers to more quickly create and synchronize testing, and more rapidly plan and execute cyber training and test events?
• Relevance – Will the effort enable cyber mission forces certification and re-certification, and training? Does the capability enable cyber range practitioners to more rapidly reconfigure networks? Does the capability increase range availability to conduct relevant training based upon realistic design of cyber environments?
• Analytics – Will the effort enable cyber practitioners to better assess how well individuals, staff and/or units operate under cyber-induced degraded, denied or compromised network conditions?

Measures:
(1) Meet capacity needs to train and certify Cyber Mission Forces (CMF) teams through FY2016.
(2) Complete all planned lifecycle modernization upgrades for FY2016.
(3) Initiate project to enable hybrid communications transport circuit solution & transition eligible JIOR communication circuits from Defense Research and Engineering Network – Defense Information Systems Network (multi-year project).
(4) Initiate project to peer the Joint IO Range and the Joint Mission Environment Test Capability 2.0 (JMETC 2.0) in order to leverage each other's assets/capabilities.
(5) Host Cyber Guard/Cyber Flag events with less than two priority-1 (urgent fix required) and three priority-2 (immediate fix) problem trouble reports per event.
(6) Complete DoD Architecture Framework (DODAF) Viewpoint surveys and documentation in FY15. Use DODAF findings to vet designs for a virtual mil-ops cyber range with enterprise stakeholders.
(7) Work towards automating manual paper-driven planning processes in order to reduce event planning timeline.
(8) Leverage automation to progress towards reducing network reconfiguration time to maximize environment use and reuse of Defense Enterprise Cyber Range Environment (DECRE) ranges.
(9) Field Live Laboratory Advanced Visual Analytics (LAVA) to users of the JIOR.