Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Operational Test and Evaluation, Defense	Date: May 2017
Appropriation/Budget Activity 0460: *Operational Test and Evaluation, Defense* / BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0605118OTE / *Operational Test and Evaluation (OT&E)*

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
Total Program Element	90.673	76.838	80.772	83.503	-	83.503	85.397	86.803	88.620	90.499	Continuing	Continuing
0605118OTE: *OT&E*	90.673	76.838	80.772	83.503	-	83.503	85.397	86.803	88.620	90.499	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Director of Operational Test and Evaluation (DOT&E) was created by Congress in 1983. The Director is responsible under Title 10 for policy and procedures for all aspects of Operational Test and Evaluation (OT&E) within the Department of Defense (DoD). Particular focus is given to OT&E that supports major weapon system production decisions for acquisition programs included on the Office of Secretary of Defense Test and Evaluation Oversight List that is prepared and approved annually. Generally, there are about 300 programs on the oversight list including all Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS). MDAPs may not proceed beyond low-rate initial production (BLRIP) until OT&E of the program is complete. DOT&E is involved early in the planning phase of each program to ensure adequate testing is planned and executed. Key elements of DOT&E's oversight authority include:

- Approve component Test and Evaluation Master Plans (TEMPS).
- Approve component OT&E Test Plans (TPs).
- Oversee Military Department preparation and conduct of field operational tests; analysis and evaluation of the resultant test data; the assessment of the adequacy of the executed test and evaluation programs; and assessment of the operational effectiveness and suitability of the weapon systems.
- Report results of OT&E that supports BLRIP decisions to the Secretary of Defense and Congress, as well as providing an annual report summarizing all OT&E activities and the adequacy of test resources within DoD during the previous fiscal year.
- Review and make recommendations to the Secretary of Defense on all budgetary and financial matters related to OT&E, including operational test facilities, resources and ranges.

DOT&E also oversees and resources OT&E community efforts to plan and execute joint operational evaluations of information assurance and interoperability (IA and IOP) of fielded systems and networks during major Combatant Command (CCMD) and Service exercises, and reports the trends and findings in the annual report.

DOT&E is also involved in increasing the capacity to access realistically advanced cyber warfare capabilities to keep pace with heightened demand for their capabilities, advancing technologies and the growing cyber threat.

This Program Element includes funds to obtain Federally Funded Research and Development Center (FFRDC) support in performing the described tasks, travel funds to carry out oversight of the OT&E and IA and IOP programs, funds for Service teams performing information assurance and interoperability assessments during exercises, administrative support services, DFAS support, and engineering and technical support services related to the conduct of operational test and evaluation and exercise assessments.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Operational Test and Evaluation, Defense	Date: May 2017
Appropriation/Budget Activity 0460: *Operational Test and Evaluation, Defense* / BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0605118OTE / *Operational Test and Evaluation (OT&E)*

B. Program Change Summary ($ in Millions)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	76.838	78.047	80.129	-	80.129
Current President's Budget	76.838	80.772	83.503	-	83.503
Total Adjustments	0.000	2.725	3.374	-	3.374
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program increases for Cyber Testing	-	-	3.374	-	3.374
• Cybersecurity Assessments	-	2.725	-	-	-

Change Summary Explanation

AMENDED BUDGET REQUEST JUSTIFICATION: $2.725 million is required to address emergency warfighting readiness requirements
This increase is for Cybersecurity Assessments including funding three commercially available exploits to help DoD Red Teams portray Tier 3 cyber adversaries; funding and configuring three Cross Domain Solutions (CDS) for cybersecurity testing to identify vulnerabilities in fielded systems and acquisition programs, identify mitigation strategies, and promulgate efficient test guidance; deploying a new platform to improve situational awareness and control of five DoD Red Teams.

$3.374 million in FY 2018 is to develop testing standards, policies, and practices for cyber payloads.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Operational Test and Evaluation, Defense			Date: May 2017
Appropriation/Budget Activity 0460 / 6	R-1 Program Element (Number/Name) PE 0605118OTE / *Operational Test and Evaluation (OT&E)*	Project (Number/Name) 0605118OTE / *OT&E*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
0605118OTE: *OT&E*	90.673	76.838	80.772	83.503	-	83.503	85.397	86.803	88.620	90.499	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Director of Operational Test and Evaluation (DOT&E) was created by Congress in 1983. The Director is responsible under Title 10 for policy and procedures for all aspects of Operational Test and Evaluation (OT&E) within the Department of Defense (DoD). Particular focus is given to OT&E that supports major weapon system production decisions for acquisition programs included on the Office of Secretary of Defense Test and Evaluation Oversight List that is prepared and approved annually. Generally, there are about 300 programs on the oversight list including all Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS). MDAPs may not proceed beyond low-rate initial production (BLRIP) until OT&E of the program is complete. DOT&E is involved early in the planning phase of each program to ensure adequate testing is planned and executed. Key elements of DOT&E's oversight authority include:

- The approval of component Test and Evaluation Master Plans (TEMPS).
- The approval of component OT&E Test Plans (TPs).
- Oversight of Military Department preparation and conduct of field operational tests; analysis and evaluation of the resultant test data; the assessment of the adequacy of the executed test and evaluation programs; and assessment of the operational effectiveness and suitability of the weapon systems.
- Reporting results of OT&E that support BLRIP decisions to the Secretary of Defense and Congress, as well as providing an annual report summarizing all OT&E activities and the adequacy of test resources within DoD during the previous fiscal year.
- The review and make recommendations to the Secretary of Defense on all budgetary and financial matters related to OT&E, including operational test facilities, resources and ranges.

DOT&E also oversees and resources OT&E community efforts to plan and execute joint operational evaluations of information assurance and interoperability (IA and IOP) of fielded systems and networks during major Combatant Command (CCMD) and Service exercises, and reports the trends and findings in the annual report.

DOT&E is also involved in increasing the capacity to access realistically advanced cyber warfighting capabilities to keep pace with heightened demand for those capabilities, advancing technologies and the growing cyber threat.

This Program Element includes funds to obtain Federally Funded Research and Development Center (FFRDC) support in performing the described tasks, travel funds to carry out oversight of the OT&E and IA and IOP programs, funds for Service teams performing information assurance and interoperability assessments during exercises, administrative support services, DFAS support, and engineering and technical support services related to the conduct of operational test and evaluation and exercise assessments.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Operational Test and Evaluation, Defense		Date: May 2017
Appropriation/Budget Activity 0460 / 6	**R-1 Program Element (Number/Name)** PE 0605118OTE / *Operational Test and Evaluation (OT&E)*	**Project (Number/Name)** 0605118OTE / *OT&E*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Operational Test and Evaluation	76.838	80.772	83.503

FY 2016 Accomplishments:
Operational Test and Evaluation Oversight

This effort is in direct support of the Director's Title 10 responsibilities and is a continuing effort. Funding for FY 2016 provides Operational Test and Evaluation inputs for Test and Evaluation Master Plans, Test Plans, System Acquisition Reports, Defense Acquisition Executive Summary Reports for those programs designated for oversight by DOT&E and OUSD(AT&L). Key elements of DOT&E oversight authority are identified in Calendar Year 2016 Office of the Secretary of Defense Test and Evaluation Oversight List.

Cybersecurity Evaluations

DOT&E sponsored seven Combatant Command (CCMD) and two Service cybersecurity exercise assessments in FY 2016. In addition to the nine exercise assessments, DOT&E performed two assessments during visits to operational sites not involved in an exercise. All DOT&E-sponsored assessments included a "fix" phase during which DOT&E-funded cybersecurity experts helped CCMD and Service personnel address critical cybersecurity vulnerabilities. As part of our new Cyber Readiness Campaigns (CRCs), DOT&E worked with U.S. Pacific Command, U.S. Northern Command, U.S. Strategic Command, U.S. European Command, and U.S. Southern Command to evaluate a larger spectrum of cybersecurity related issues than is possible during a short exercise. The CRCs included more frequent and focused assessment events, and they helped commands address persistent, mission-critical cybersecurity vulnerabilities. To enable more threat-representative and longer-duration adversary portrayal, DOT&E initiated a Persistent Cyber Opposing Force (PCO) capability as part of U.S. Pacific Command's CRC as well as at U.S. Northern Command. DOT&E worked with U.S. Cyber Command to expand the use of PCOs to better understand and address our network vulnerabilities, to be more threat representative, and to allow more efficient use of limited cyber red team assets. To support cybersecurity assessments of live DoD networks, DOT&E conducted lab-based cyber testing of cross-domain solutions (CDSs) and programmable logic controllers (PLCs). These are critical components in many DoD systems and networks, and DOT&E's testing resulted in recommendations to improve CDS and PLC security and test procedures. Using personnel with advanced cybersecurity expertise, DOT&E conducted evaluations of a small number of offensive cyber capabilities in direct support of the capabilities' sponsor. DOT&E transmitted critical findings to DoD leadership along with recommended actions to improve DoD's cybersecurity posture. DOT&E's FY 2016 cybersecurity evaluations included trend analyses across prior year results, both within and across CCMDs.

FY 2017 Plans:
Operational Test and Evaluation Oversight

Exhibit R-2A, RDT&E Project Justification: FY 2018 Operational Test and Evaluation, Defense		Date: May 2017
Appropriation/Budget Activity 0460 / 6	**R-1 Program Element (Number/Name)** PE 0605118OTE / *Operational Test and Evaluation (OT&E)*	**Project (Number/Name)** 0605118OTE / *OT&E*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
This effort is in direct support of the Director's Title 10 responsibilities and is a continuing effort. Funding for FY 2017 provides Operational Test and Evaluation inputs for Test and Evaluation Master Plans, Test Plans, System Acquisition Reports, Defense Acquisition Executive Summary Reports for those programs designated for oversight by DOT&E and OUSD(AT&L). Key elements of DOT&E oversight authority are identified in Calendar Year 2017 Office of the Secretary of Defense Test and Evaluation Oversight List. Cybersecurity Evaluations DOT&E plans to sponsor approximately 10 CCMD and Service cybersecurity assessments and CRCs in FY 2017, each including a "fix" phase as described above. DOT&E plans to continue working with the CCMDs and Services to develop multi-year plans for exercise cyber assessments and CRC events. These plans will focus on assessing the CCMD or Service's ability to complete missions in a contested cyber environment. To support threat-representative assessments, and to enable continuous improvement of DoD's cybersecurity posture, DOT&E will continue to work with U.S. Cyber Command to establish a PCO capability for all CCMDs and Services. Primary objectives for DOT&E's assessments in FY 2017 include the portrayal of advanced nation-state cyber threats and the assessment of operational missions during realistic cyber attacks. DOT&E will assess Cyber Protection Teams when they participate during PCO, CRC or exercise events. DOT&E will continue to develop techniques to efficiently and effectively assess offensive cyber capabilities, and conduct timely evaluations of these capabilities. DOT&E will use the DoD Enterprise Cyber Range Environment (DECRE) and other lab and cyber range assets to support events, for added threat realism. DOT&E will transmit critical findings to DoD leadership along with recommended actions to improve DoD's cybersecurity posture. FY 2017 evaluations will include trend analyses across prior year results, both within and across CCMDs.			
FY 2018 Plans: Operational Test and Evaluation Oversight This effort is in direct support of the Director's Title 10 responsibilities and is a continuing effort. Funding for FY 2018 provides Operational Test and Evaluation inputs for Test and Evaluation Master Plans, Test Plans, System Acquisition Reports, Defense Acquisition Executive Summary Reports for those programs designated for oversight by DOT&E and OUSD(AT&L). Key elements of DOT&E oversight authority are identified in Calendar Year 2018 Office of the Secretary of Defense Test and Evaluation Oversight List. Cybersecurity Evaluations			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Operational Test and Evaluation, Defense		Date: May 2017
Appropriation/Budget Activity 0460 / 6	**R-1 Program Element (Number/Name)** PE 0605118OTE / *Operational Test and Evaluation (OT&E)*	**Project (Number/Name)** 0605118OTE / *OT&E*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
DOT&E will oversee and resource approximately 10 CCMD and Service assessments in FY 2018, each including a "fix" phase. Pending CCMD and Service agreement, DOT&E plans to conduct CRC events with all of the CCMDs and Services. Each CRC will include frequent assessments focused on new cybersecurity technologies or procedures to address problems identified in prior assessments. CRCs will culminate in a capstone event during a major exercise that evaluates the cybersecurity of critical missions, as improved by the new technologies and procedures. Using the PCO, DOT&E will continue to work with the CCMDs and cyber red teams to increase the portrayal of advanced nation-state cyber threats. The goal is to have the majority of assessments in FY 2018 include advanced threats that stress critical missions. DOT&E will assess Cyber Protection Teams when they participate during PCO, CRC or exercise events. DOT&E will continue to develop techniques to efficiently and effectively assess offensive cyber capabilities, and conduct timely evaluations of these capabilities. DOT&E will use the DoD Enterprise Cyber Range Environment (DECRE) and other lab and cyber range assets to support events, for added threat realism. DOT&E will transmit critical findings to DoD leadership along with recommended actions to improve DoD's cybersecurity posture. FY 2018 evaluations will include trend analyses across prior year results, both within and across CCMDs and Services. In FY 2018 DOT&E will develop testing standards, policies, and practices for cyber payloads.			
Accomplishments/Planned Programs Subtotals	76.838	80.772	83.503

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Performance Measure: Percentage of required operational test planning documents, assessments, and reports applicable to acquisition programs on the OSD Test and Evaluation Oversight List and other special interest programs/legacy systems that are completed and delivered to the appropriate decision makers on time.
The on-time completion rate was computed on the basis of the number of required products that were submitted within established time standards relative to the total number of such products that fell due during the fiscal year. Products included in the measure include beyond low-rate initial production reports, Test Plans, and Test and Evaluation Master Plans for operational test and evaluation oversight as well as assessment plans, "quick look" reports, and final reports for the information assurance and interoperability testing associated with scheduled test events.