Exhibit R-2, **RDT&E Budget Item Justification:** PB 2012 Air Force									**DATE:** February 2011	
APPROPRIATION/BUDGET ACTIVITY 3600: *Research, Development, Test & Evaluation, Air Force* BA 6: *RDT&E Management Support*					**R-1 ITEM NOMENCLATURE** PE 0804731F: *GENERAL SKILL TRAINING*					

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	1.399	1.544	1.510	-	1.510	1.292	1.356	1.375	1.400	Continuing	Continuing
665297: *Technical Training Information Systems*	1.399	1.544	1.510	-	1.510	1.292	1.356	1.375	1.400	Continuing	Continuing

A. Mission Description and Budget Item Justification

The DoD Cyber Crime Center (DC3) is a service organization that provides on demand state-of-the-art electronic forensic services and cyber investigative and operational support to the Department of Defense (DoD). DC3 also provides leadership as a DoD center of excellence in processing an analyzing digital evidence.
It provides professional special investigative services for the protection of DoD people, investigations, operations, material and critical infrastructures worldwide.
The DC3's objective is to support and address the proliferation of cyber crimes within or directed at the DoD. Within DC3, the DoD Cyber Crime Institute (DCCI) develops the foundation for accepted standards and practices based on valid research, science, and law with innovative ideas and methods. It serves as a resource for sound research to produce unique tools and procedures for the DoD law enforcement, counter terrorism, counterintelligence, force protection, information assurance, information operations and war fighting communities. It strives to develop national electronic forensics standards, cyber investigative tools and techniques, effective plans, policies and procedures and implement a knowledge management system. It provides the DoD community with analytical services and produces relevant intelligence reports, criminal intelligence reports and cyber investigation trend analyses. It focuses on new issues facing the DoD critical infrastructure protection efforts and those facing the cyber investigative discipline. DC3 must continue to expand its capabilities and continue to develop effective plans, policies, and procedures for addressing cybercrime and electronic forensic needs in DoD both now and in the future. The primary goal is to ensure the DoD has the ability to successfully perform its mission of electronic media processing and analysis in the future.

This program is in Budget Activity 6, RDT&E Management Support because this budget activity includes research, development, test and evaluation efforts and funds to sustain and/or modernize the installations or operations required for general research, development, test and evaluation.

B. Program Change Summary ($ in Millions)

	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total
Previous President's Budget	1.450	1.544	1.581	-	1.581
Current President's Budget	1.399	1.544	1.510	-	1.510
Total Adjustments	-0.051	-	-0.071	-	-0.071
• Congressional General Reductions		-			
• Congressional Directed Reductions		-			
• Congressional Rescissions	-	-			
• Congressional Adds		-			
• Congressional Directed Transfers		-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.051	-			
• Other Adjustments	-	-	-0.071	-	-0.071

Exhibit R-2A, RDT&E Project Justification: PB 2012 Air Force									DATE: February 2011	

APPROPRIATION/BUDGET ACTIVITY 3600: *Research, Development, Test & Evaluation, Air Force* BA 6: *RDT&E Management Support*				R-1 ITEM NOMENCLATURE PE 0804731F: *GENERAL SKILL TRAINING*				PROJECT 665297: *Technical Training Information Systems*		

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
665297: *Technical Training Information Systems*	1.399	1.544	1.510	-	1.510	1.292	1.356	1.375	1.400	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The DoD Cyber Crime Center (DC3) is a service organization that provides on demand state-of-the-art electronic forensic services and cyber investigative and operational support to the Department of Defense (DoD). DC3 also provides leadership as a DoD center of excellence in processing an analyzing digital evidence. It provides professional special investigative services for the protection of DoD people, investigations, operations, material and critical infrastructures worldwide. The DC3's objective is to support and address the proliferation of cyber crimes within or directed at the DoD. Within DC3, the DoD Cyber Crime Institute (DCCI) develops the foundation for accepted standards and practices based on valid research, science, and law with innovative ideas and methods. It serves as a resource for sound research to produce unique tools and procedures for the DoD law enforcement, counter terrorism, counterintelligence, force protection, information assurance, information operations and war fighting communities. It strives to develop national electronic forensics standards, cyber investigative tools and techniques, effective plans, policies and procedures and implement a knowledge management system. It provides the DoD community with analytical services and produces relevant intelligence reports, criminal intelligence reports and cyber investigation trend analyses. It focuses on new issues facing the DoD critical infrastructure protection efforts and those facing the cyber investigative discipline. DC3 must continue to expand its capabilities and continue to develop effective plans, policies, and procedures for addressing cybercrime and electronic forensic needs in DoD both now and in the future. The primary goal is to ensure the DoD has the ability to successfully perform its mission of electronic media processing and analysis in the future. Without funding, critical projects will be terminated. The DoD's ability to process digital evidence in a future environment of increasing case loads that have a large amount of data that is also hidden by sophisticated techniques will be greatly degraded.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total
Title: Cyber Crime *Description:* Develop plans/policies/procedures for cybercrime issues *FY 2010 Accomplishments:* Begin conducting electronic forensics and cyber investigations (Digital evidence processing, special investigation services, etc). *FY 2011 Plans:* Continue conducting electronic forensics and cyber investigations (Digital evidence processing, special investigation services, etc). *FY 2012 Base Plans:*	1.399	1.544	1.510	-	1.510

Exhibit R-2A, RDT&E Project Justification: PB 2012 Air Force		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 3600: *Research, Development, Test & Evaluation, Air Force* BA 6: *RDT&E Management Support*	**R-1 ITEM NOMENCLATURE** PE 0804731F: *GENERAL SKILL TRAINING*	**PROJECT** 665297: *Technical Training Information Systems*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total
Begin conducting electronic forensics and cyber investigations (Digital evidence processing, special investigation services, etc). ***FY 2012 OCO Plans:***					
Accomplishments/Planned Programs Subtotals	1.399	1.544	1.510	-	1.510

C. Other Program Funding Summary ($ in Millions)

Line Item	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
• N/A:	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing

D. Acquisition Strategy

Not applicable

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.