

UNCLASSIFIED

PE NUMBER: 0804731F
 PE TITLE: GENERAL SKILL TRAINING

| | |
|---|-------------------------|
| Exhibit R-2, RDT&E Budget Item Justification | DATE May 2009 |
|---|-------------------------|

| | |
|--|--|
| BUDGET ACTIVITY 06 RDT&E Management Support | PE NUMBER AND TITLE 0804731F GENERAL SKILL TRAINING |
|--|--|

| | Cost (\$ in Millions) | FY 2008 Actual | FY 2009 Estimate | FY 2010 Estimate | FY 2011 Estimate | FY 2012 Estimate | FY 2013 Estimate | FY 2014 Estimate | FY 2015 Estimate | Cost to Complete | Total |
|------|--|-------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|-------|
| | Total Program Element (PE) Cost | 2.904 | 0.000 | 1.450 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | Continuing | TBD |
| 4980 | Research and Development of Computer Forensic Anaylst Tools | 2.904 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | Continuing | TBD |
| 5297 | Technical Training Information Systems | 0.000 | 0.000 | 1.450 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |

(U) 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 and 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.

This program is in Budget Activity 6 - Management and Support

Exhibit R-2, RDT&E Budget Item Justification

DATE

May 2009

BUDGET ACTIVITY

06 RDT&E Management Support

PE NUMBER AND TITLE

0804731F GENERAL SKILL TRAINING

(U) **B. Program Change Summary (\$ in Millions)**

| | <u>FY 2008</u> | <u>FY 2009</u> | <u>FY 2010</u> |
|---|----------------|----------------|----------------|
| (U) Previous President's Budget | 2.904 | 0.000 | 1.475 |
| (U) Current PBR/President's Budget | 2.904 | 0.000 | 1.450 |
| (U) Total Adjustments | 0.000 | 0.000 | |
| (U) Congressional Program Reductions | | | |
| Congressional Rescissions | | | |
| Congressional Increases | | | |
| Reprogrammings | | | |
| SBIR/STTR Transfer | | | |
| (U) <u>Significant Program Changes:</u> | | | |

Exhibit R-2a, RDT&E Project Justification

DATE
May 2009

| | | | | | | | | | | |
|--|-------------------|---------------------|---------------------|---------------------|---|---------------------|---------------------|---|---------------------|-------|
| BUDGET ACTIVITY 06 RDT&E Management Support | | | | | PE NUMBER AND TITLE 0804731F GENERAL SKILL TRAINING | | | PROJECT NUMBER AND TITLE 4980 Research and Development of Computer Forensic Anaylst Tools | | |
| Cost (\$ in Millions) | FY 2008 Actual | FY 2009 Estimate | FY 2010 Estimate | FY 2011 Estimate | FY 2012 Estimate | FY 2013 Estimate | FY 2014 Estimate | FY 2015 Estimate | Cost to Complete | Total |
| 4980 Research and Development of Computer Forensic Anaylst Tools | 2.904 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | Continuing | TBD |
| Quantity of RDT&E Articles | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |

(U) A. Mission Description and Budget Item Justification

Develop national electronic forensics standards, cyber investigative tools and techniques, effective plans, policies and procedures and implement a knowledge management system. Provides the DoD community with analytical services and produces relevant intelligence reports, criminal intelligence reports and cyber investigation trend analyses. Focuses on new issues facing the DoD critical infrastructure protection efforts and those facing the cyber investigative discipline. Effort 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.

(U) B. Accomplishments/Planned Program (\$ in Millions)

| | <u>FY 2008</u> | <u>FY 2009</u> | <u>FY 2010</u> |
|--|----------------|----------------|----------------|
| (U) Accomplished/Planned Programs | | | |
| (U) Next Generation Electronic Media Analysis System | 0.731 | | |
| (U) Damaged Storage Device Data Recovery Tools | 0.600 | | |
| (U) Knowledge Management System | 0.540 | | |
| (U) Vulnerability Assessment Environment (V.A.E.) | 0.452 | | |
| (U) Fused Analysis System/Data Analysis Tools | 0.581 | | |
| (U) Total Cost | 2.904 | 0.000 | 0.000 |

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

| | <u>FY 2008</u> | <u>FY 2009</u> | <u>FY 2010</u> | <u>FY 2011</u> | <u>FY 2012</u> | <u>FY 2013</u> | <u>FY 2014</u> | <u>FY 2015</u> | <u>Cost to</u> | <u>Total Cost</u> |
|-----------------------|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-------------------|
| | <u>Actual</u> | <u>Estimate</u> | <u>Complete</u> | |
| (U) Other Procurement | 0.572 | 0.290 | 0.298 | 0.609 | | | | | Continuing | TBD |

(U) D. Acquisition Strategy

All major contracts were awarded sole source contract due to the sensitivity of the technologies involved.

Exhibit R-2a, RDT&E Project Justification

DATE
May 2009

| | | | | | | | | | | |
|---|-------------------|---------------------|---------------------|---------------------|---|---------------------|---------------------|--|---------------------|-------|
| BUDGET ACTIVITY 06 RDT&E Management Support | | | | | PE NUMBER AND TITLE 0804731F GENERAL SKILL TRAINING | | | PROJECT NUMBER AND TITLE 5297 Technical Training Information Systems | | |
| Cost (\$ in Millions) | FY 2008 Actual | FY 2009 Estimate | FY 2010 Estimate | FY 2011 Estimate | FY 2012 Estimate | FY 2013 Estimate | FY 2014 Estimate | FY 2015 Estimate | Cost to Complete | Total |
| 5297 Technical Training Information Systems | 0.000 | 0.000 | 1.450 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| Quantity of RDT&E Articles | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |

(U) 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 and 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.

(U) B. Accomplishments/Planned Program (\$ in Millions)

| | <u>FY 2008</u> | <u>FY 2009</u> | <u>FY 2010</u> |
|--|----------------|----------------|----------------|
| (U) Develop plans/policies/procedures for cybercrime issues | | | 0.350 |
| (U) Electronic forensics and cyber investigations (Digital evidence processing, special investigation services, etc) | | | 1.100 |
| (U) Total Cost | 0.000 | 0.000 | 1.450 |

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

| | <u>FY 2008</u> | <u>FY 2009</u> | <u>FY 2010</u> | <u>FY 2011</u> | <u>FY 2012</u> | <u>FY 2013</u> | <u>FY 2014</u> | <u>FY 2015</u> | <u>Cost to</u> | <u>Total Cost</u> |
|--------------------|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-------------------|
| | <u>Actual</u> | <u>Estimate</u> | <u>Complete</u> | |
| (U) Not applicable | | | | | | | | | | |

(U) D. Acquisition Strategy

Not applicable