

Exhibit R-2, RDT&E Budget Item Justification						Date: February 2006	
APPROPRIATION/BUDGET ACTIVITY	R-1 ITEM NOMENCLATURE						
RDT&E, Defense Wide (0400), Budget Activity 7	0305125D8Z/CRITICAL INFRASTRUCTURE PROTECTION (CIP)						
COST (\$ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	27.260	12.166	12.422	13.090	13.080	13.284	13.519
Critical Infrastructure Protection Project 125	27.260	12.166	12.422	13.090	13.080	13.284	13.519

A. Mission Description and Budget Item Justification

Homeland Security Presidential Directive #7 (HSPD-7), signed by President Bush on 17 December 2003, established national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks. In September 2003, the Deputy Secretary of Defense transferred oversight of the Defense Critical Infrastructure Program to the Office of the Assistant Secretary of Defense for Homeland Defense.

The Defense Critical Infrastructure Program is an integrated risk management program designed to assure the continuous availability of networked infrastructure assets, whether owned or operated by the Department of Defense or private industry, that are critical to executing military missions. Activities include the identification, assessment, monitoring, and risk management of cyber and physical infrastructure assets critical to the execution of the National Military Strategy.

Effective critical infrastructure protection results from actions taken to prevent, remediate, or mitigate the risks resulting from identified susceptibilities. Risk is managed by balancing probability of threat, impact of loss, and extent of the susceptibility. Depending on the risk, protection actions can include changes in tactics or procedures, added redundancy, selection of other assets to provide a similar service, isolation or hardening, or physically guarding, thus making the affected critical asset a hard target and improving overall critical infrastructure reliability. From an infrastructure protection perspective, this approach enables the achievement of warfighter operational goals through assured continuity of combat support and core Defense business processes, and assists in the restoration of capabilities should a disruption occur.

* Previous funding in the Navy RDT&E.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification

Date: February 2006

B. Program Change Summary: Additional funds were reprogrammed to accelerate the development of mission assurance objectives for direct application in the Global War on Terrorism and Enduring Iraqi Freedom theaters as well as enhancing readiness of supporting domestic infrastructure. This acceleration will further the identification, prioritization and management of risk associated with critical assets supporting Department of Defense mission objectives both at home and in forward deployed areas.

COST (\$ in Millions)	FY 2005	FY 2006	FY 2007
Previous President's Budget	28.367	11.363	12.229
Current BES/President's Budget	27.260	12.159	12.422
Total Adjustments:			
Congressional program reductions			
Congressional rescissions			
Congressional increases			
Reprogrammings			
SBIR/SSSTR Transfer			
Program Adjustment	-1.107	.796	.193

C. Other Program Funding Summary:

COST (\$ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
O&M,DW 0902198D8Z	10.7	23.3	23.1	11.9	12.0	12.4	12.7

D. Acquisition Strategy: N/A

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification

Date: February 2006

E. Performance Metrics:

FY 2005 Performance Metrics

- Conducted Defense Critical Infrastructure Program pilot assessments in coordination with the Joint Staff
- Identified Service assets specific to Department of Defense missions identified by the Combatant Commands
- Developed, coordinated and obtained formal signature of Department of Defense Directive 3020.40, "Defense Critical Infrastructure Program."

FY 2006 Performance Metrics

- Publish a Department of Defense standard methodology to identify critical assets
- Publish infrastructure standards for use by existing assessment programs across Department of Defense
- Implement a self assessment capability based on published infrastructure standards for use by Department of Defense asset owners and industry assets supporting Department of Defense missions

FY 2007 – FY 2011 Performance Metrics

- Develop a risk management methodology to apply to all identified critical assets
- Develop a prioritization methodology to substantiate investment in risk management recommendations
- Perform infrastructure dependency assessments and evaluate results to reduce any recurring susceptibilities

UNCLASSIFIED

R1 Shopping List Item No. 186

Page 3 of 10

585

Exhibit R-2a, RDT&E Project Justification						Date: February 2006	
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT		PROJECT NAME AND NUMBER				
RDT&E, Defense Wide (0400), BA 7	0305125D8Z		CRITICAL INFRASTRUCTURE PROTECTION (CIP)				
COST (\$ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Critical Infrastructure Protection Project 125	27.260	12.166	12.422	13.090	13.080	13.284	13.519

A. Mission Description and Budget Item Justification:

The Defense Critical Infrastructure Program (DCIP) is a Department of Defense (DoD) risk management program that seeks to ensure resiliency of defense critical infrastructure, which includes DoD and non-DoD, domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining United States military operations on a global basis. DCIP is directed by the Assistant Secretary of Defense for Homeland Defense [ASD(HD)] and managed by the Director for Critical Infrastructure Protection (CIP). DoD Directive 3020.40, 19 August 2005, establishes policy and assigns responsibilities for the DCIP.

The identification, prioritization, assessment, and assurance of defense critical infrastructure is managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect defense critical infrastructure related sensitive information.

Combatant Commands (COCOMs) are responsible for identifying critical warfighting missions, priorities, capabilities, and forces to meet the National Military Strategy. Service Component Commanders and Military Departments identify and prioritize assets required by COCOMs to execute the critical warfighting missions. The Defense Sector lead agents are responsible for identifying the specific functions, systems, assets (DoD and non-DoD owned), and interdependencies within the Defense Sector infrastructure networks supporting the identified critical missions.

DoD has ten (10) functional areas that provide support to COCOMs, Service Component Commanders, and Military Departments. Each functional area has a Defense Sector Lead Agent as identified in DoDD3020.40. These functional areas are as follows: defense industrial base (DIB); financial services; global information grid (GIG); health affairs; intelligence, surveillance, and reconnaissance (ISR); logistics; personnel; public works; space; and transportation.

In addition, DCIP manages specific analytic efforts in the identification and maintenance of specific inter- and intra-dependencies DoD has on the foundational commercial infrastructure networks supporting the identified critical missions. Specific analytic efforts are focused within six (6) commercial infrastructure areas: energy (electric power, natural gas); chemicals; transportation; telecommunications; water; and petroleum, oil, lubricants (POL).

Exhibit R-2a, RDT&E Project Justification

Date: February 2006

B. Program Change Summary

	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	14.000	5.463	5.343

Understanding Risks Through Analysis and Assessment:

FY 2005: The program has:

- Developed a Department of Defense (DoD) standard methodology to identify critical assets
- Developed standards and benchmarks for DoD infrastructure assessments
- Conducted pilot Defense Critical Infrastructure Program (DCIP) assessments on identified and prioritized critical assets to quantify associated risk as well as validate the standards and benchmarks

FY 2006: The program will:

- Institute a DoD standard methodology to identify critical assets
- Institute standards and benchmarks for DoD infrastructure assessments.
- Develop comprehensive training material to support incorporation of infrastructure assessment standards into existing assessment programs.
- Develop, test, and validate a remote self-assessment tool to provide the Service Component Commanders and the Defense Sectors/Agencies a more responsive, efficient assessment capability.
- Institute standardized DCIP methodology for conducting mission area analysis, foundational infrastructure analysis, and Defense Sector characterization.

FY 2007: The program will:

- Establish a standard risk management methodology to apply to all identified critical assets.

Exhibit R-2a, RDT&E Project Justification	Date: February 2006
--	----------------------------

	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	3.624	1.572	.955

Prepare, Plan and Respond to Incidents:

FY 2005: The program has:

- Responded to mission-focused analysis tasks, quick turn around requests for National Special Security Events, and DCIP community tasks directly supporting the Global War on Terror, Operation Iraqi Freedom and Operation Enduring Freedom.
- Provided an effective response capability to identify potential mission impacts to Department of Defense (DoD) from actual or anticipated events against United States or host nation infrastructure.
- Developed an all-hazards Continuity of Operations (COOP) plan to sustain Defense Critical Infrastructure Program (DCIP) capabilities in the event of a disaster

FY 2006: The program will:

- Respond to mission-focused analysis tasks, quick turn around requests for National Special Security Events, and DCIP community tasks directly supporting the Global War on Terror, Operation Iraqi Freedom and Operation Enduring Freedom.
- Provide an effective response capability to identify potential mission impacts to DoD from actual or anticipated events against U.S. or host nation infrastructure.
- Implement an all-hazards Continuity of Operations (COOP) plan to sustain DCIP capabilities in event of a disaster.
- Institute a monitoring and reporting capability that will improve overall responsiveness to threats associated with DCIP assets.

FY 2007: The program will:

- Perform trend analysis and develop remediation and mitigation options for addressing risks identified as part of the assessment process.
- Support taskings for critical asset or infrastructure data in support of designated National Security Special Events, validated requests from Combatant Commands, and other quick-response taskings.
- Provide an effective response capability to identify potential mission impacts to DoD from actual or anticipated events against U.S. or host nation infrastructure.

Exhibit R-2a, RDT&E Project Justification	Date: February 2006
--	----------------------------

	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	6.051	2.776	3.712

Provide Program Support and Integration:

FY 2005: The program has:

- Developed a monitoring and reporting capability that will improve overall responsiveness to potential threatening situations associated with DCIP assets.
- Provided liaisons to coordinate with other government agencies to further information sharing and leveraging of Critical Infrastructure Protection (CIP) information and capabilities across the homeland security interagency community.
- Provided a liaison focused on establishing cooperative agreements with the international community with related CIP interests relevant to those of the United States DoD.
- Began development of a top-down framework based upon reference standards to address global Enterprise Architecture (EA) to include: Development of a comprehensive EA Strategy to include: appropriate subordinates strategies to implement the EA program; a comprehensive architecture framework; concept papers on EA implementation processes; a Portfolio Management (PfM) process; a Configuration Management and Control (CCM) process; functional and technical process flow templates that map to the Defense Critical Infrastructure Program (DCIP) mission, goals, and objectives; appropriate EA documentation; an EA awareness strategy; and provide Systems Engineering expertise, and Enterprise Architecture expertise.

Exhibit R-2a, RDT&E Project Justification

Date: February 2006

FY 2006: The program will:

- Institute a monitoring and reporting capability that will improve overall responsiveness to potential threatening situations associated with DCIP assets.
- Identify standard data sources for infrastructure data to be used across DoD.
- Determine Education and Training requirements to ensure a cohesive DCIP effort and to accomplish program goals and objectives consistently across the community.
- Develop and implement a responsive Research, Development (R&D) and Technical Integration capability to evaluate the potential for new, technologies to provide added capability and value into the DCIP. This capability will include the development of a formal, requirements-driven process for considering and evaluating technical capabilities, data sets, assessment methodologies and other pertinent activities relevant to DCIP.
- Continue development of a top-down framework based upon reference standards to address global Enterprise Architecture (EA). Develop a comprehensive EA Strategy to include: appropriate subordinates strategies to implement the EA program; a comprehensive architecture framework; concept papers on EA processes; a Portfolio Management (PfM) process; a Configuration Management and Control (CCM) process; functional and technical process flow templates that map to DCIP mission, goals, and objectives; appropriate EA documentation; an EA awareness strategy; and provide Systems Engineering expertise, EA expertise, and support to the OASD(HD) CIP staff, the DCIP EA Working Group, and to the DCIP community, as required.

FY 2007: The program will:

- Develop, leverage, maintain, and enhance tools and data sets based on requirements derived from the DCIP community and the output of assessments performed on the Defense Industrial Base assets.
- Review, validate, prioritize, and develop DCIP concepts focused on concept development for military mission assurance; infrastructure remediations; DCIP assessment tools and methods; operations centers; techniques to respond to infrastructure disruptions; and multi-level security systems for advanced information sharing.
- Integrate identification, prioritization, assessment, and assurance efforts to adequately assess risk to DoD's critical missions. Track the progress of the remediation and mitigation of identified risks.
- Evaluate and prioritize concept development for military remediation; commercial infrastructure mission assurance; DCIP assessment tools and methods; decision support systems; focused operations centers; and response to infrastructure disruptions; and multi-level security systems for advanced information sharing.

Exhibit R-2a, RDT&E Project Justification	Date: February 2006
--	---------------------

	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	4.692	2.348	2.412

Enable Management Initiatives:

FY 2005: The program has:

- Recommended, drafted, reviewed, and revised documentation associated with the Defense Critical Infrastructure Program (DCIP) and mission assurance policy, strategy, and plans.
- Reviewed and validated DCIP requirements received from the DCIP community
- Begun development of DCIP metrics to ensure that program accomplishments can be measured and reported.
- Overseen the Combatant Commands, Military Services, and Defense Sector responsibilities identified in DoD Directive 3020.40.

FY 2006: The program will:

- Review and validate DCIP requirements received from the DCIP community
- Establish, implement, and manage appropriate DCIP metrics to ensure that program accomplishments can be measured and reported.
- Track assessment, remediation, and mitigation efforts for DCIP to enable a value-added determination based on increased protective measures put in place.
- Oversee the Combatant Commands, Military Services, and Defense Sector responsibilities identified in DoD Directive 3020.40.

FY 2007: The program will:

- Review and validate DCIP requirements received from the DCIP community.
- Establish, implement, and manage appropriate DCIP metrics to ensure that program accomplishments can be measured and reported.
- Track assessment, remediation, and mitigation efforts for DCIP to enable a value-added determination based on increased protective measures put in place.
- Oversee the Combatant Commands, Military Services, and Defense Sector responsibilities identified in DoD Directive 3020.40.

Exhibit R-2a, RDT&E Project Justification

Date: February 2006

C. Other Program Funding Summary: DCIP O&M funding is allocated to the Combatant Commands, Military Services, and Defense Sectors/Defense Agencies. This funding will be used by these organizations to identify critical assets supporting DoD missions using the standard methodology developed through DCIP, assessing these identified critical assets to identify critical infrastructure support, and the performance of risk management activities associated with these assessed assets.

COST (\$ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
O&M,DW 0902198D8Z	10.7	23.3	23.1	11.9	12.0	12.4	12.7

D. Acquisition Strategy: N/A

E. Major Performers: N/A