Exhibit R-2, RDT&E Budget Item Justification									Date: February 2007	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense Wide (0400), Budget Activity 7				R-1 ITEM NOMENCLATURE 0305125D8Z/CRITICAL INFRASTRUCTURE PROTECTION (CIP)						
COST ($ in Millions)	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	Cost to Complete	Total Cost
Total PE Cost	19.166	13.643	12.667	12.731	13.014	13.162	13.367	13.573	Continues	Continues
Critical Infrastructure Protection Project 125	19.166	13.643	12.667	12.731	13.014	13.162	13.367	13.573	Continues	Continues

A. Mission Description and Budget Item Justification

Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, assigns two sets of responsibilities to the Department of Defense (DoD). First, as a Federal Department and related specifically to DoD mission critical infrastructure, DoD has the responsibility to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them." Second, HSPD-7 designates DoD as the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). The Defense Industrial Base (DIB) is the DoD, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. As the SSA for the DIB, DoD is responsible for collaborating with all relevant organizations, conducting or facilitating vulnerability assessments, and encouraging risk management strategies to protect against attacks on the DIB.

HSPD-7 focuses on the national plan to secure critical infrastructure. Subsequent documents and strategies issued by DoD have expanded on this baseline to detail DoD critical infrastructure protection (CIP) efforts. The June 2005 *Strategy for Homeland Defense and Civil Support* identifies preparedness and protection of Defense Critical Infrastructure as one of the core capabilities to achieve mission assurance.

The cornerstone of DoD's approach to CIP is DoD Directive (DoDD) 3020.40, *Defense Critical Infrastructure Program (DCIP)*, signed by the Deputy Secretary of Defense in August 2005, which assigns the roles and responsibilities for implementing the DCIP. The Defense Critical Infrastructure Program (DCIP), as defined in DoDD 3020.40, is a DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

The DCIP is a DoD-wide effort, involving components from the Office of the Secretary of Defense (OSD), the Joint Staff, the Combatant Commands (COCOMs), the Military Departments and Services, the Defense Agencies and Field Activities, the National Guard Bureau, and the Defense Infrastructure Sector Leads. These DoD components and officials must work together, form partnerships, and integrate activities in order to accomplish the DCIP responsibilities identified in DoDD 3020.40.

The immense scope of infrastructures and the interdependent nature of their environment necessitate a comprehensive risk management effort. Providing complete assurance of every Defense Critical Infrastructure Asset in an all-hazards environment from all conceivable hazards is not feasible. Therefore, DoD will apply risk management practices on Defense Critical Infrastructure.

Risk management practices are applied by first performing a risk assessment to understand (1) what assets are critical to DoD missions, (2) identifying vulnerabilities to those assets, and (3) identifying threats and hazards to those assets.

Decision makers use the results of the risk assessments to determine a risk response. This response may include applying resources to fix identified vulnerabilities, change tactics or procedures, provide asset redundancy, or accept the identified risk. The risk management approach will support the prioritization of scarce resources across DoD and focus resources on these assets critical to DoD missions. 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.

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2007

B. Program Change Summary:

COST ($ in Millions)	FY 2006	FY 2007	FY 2008	FY2009
Previous President's Budget	12.166	12.422	13.090	13.080
Current BES/President's Budget	19.166	13.643	12.667	12.731
Total Adjustments:				
Congressional program reductions		-0.079	-0.423	-0.349
Congressional rescissions				
Congressional increases	7.000	1.300		
Reprogrammings				
SBIR/SSTR Transfer				
Program Adjustment	19.166	13.643	12.667	12.731

C. Other Program Funding Summary:

COST ($ in Millions)	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY2012	FY2013
O&M,DW 0902198D8Z	29.579	20.567	18.997	20.053	20.322	19.829	20.233	20.635

D. Acquisition Strategy: N/A

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2007

E. Performance Metrics:

FY 2006 Performance Metrics

- Published supporting foundation infrastructure benchmarks for use by assessment programs across the Department of Defense and Defense Industrial Base (DIB) complex..
- Developed DoD DCIP assessment training curriculum
- Published a DCIP Interim Implementation Guidance (IIG) as a bridging document to formal coordination and issuance of a DCIP DoD Instruction (DoDI).
- Established an Integrated Product Team (IPT) to work issues related to drafting and publishing a DCIP DoDI.
- Published a Department of Defense criticality methodology to identify defense critical assets.
- Conducted functional mission decomposition of two Joint Capability Areas (JCAs).
- Institutionalized an inter-agency process to identify authoritative geospatial data sources.
- Developed Knowledge Display and Aggregation System (KDAS) initial operating capability, leveraging the National Geospatial Intelligence Agency's (NGA) Palanterra system.
- Establishing web-services for Defense Sector databases with KDAS/Palanterra.
- Published the DCIP Geospatial Data Strategy.
- Initiated Independent Verification and Validation of Defense databases and tools suites used to conduct defense and commercial interdependency analysis.

FY 2007 Performance Metrics

- Coordinate and publish a DCIP DoD Instruction (DoDI).
- Incorporate DoD DCIP assessment training curriculum into established DoD education and training programs.
- Coordinate and publish the DoD criticality methodology to identify defense critical assets.
- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical assets contained on the COCOM Integrated Priority List (IPL).
- Publish the DCIP Risk Assessment Handbook.
- Continue web service integration for remaining Defense Sector databases, Combatant Command, and Military Service databases for visualization of assets in KDAS/Palanterra visualization tool to create a DCIP COP.

FY2008 Performance Metrics

- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical infrastructure assets contained on the COCOM Integrated Priority List (IPL).
- Apply risk management methodology to all identified critical assets.
- Develop a prioritization methodology to substantiate investment in risk management recommendations.
- Develop, leverage, maintain, and enhance tools and data sets based on requirements derived from the DCIP community and the output of assessments performed on Defense Industrial Base (DIB) assets.
- Develop protocols and standards to ensure interoperability of Homeland Security Information Network Components and DCIP COP for a HLS/HLD COP and situational awareness.

FY2009– FY 2013 Performance Metrics

- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical infrastructure assets per year.
- Apply risk management methodology to all identified critical assets.
- Develop, leverage, maintain, and enhance tools and data sets based on requirements derived from the DCIP community and the output of assessments performed on Defense Industrial Base (DIB) assets.

Exhibit R-2a, RDT&E Project Justification									Date: February 2007	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense Wide (0400), BA 7			PROGRAM ELEMENT 0305125D8Z			PROJECT NAME AND NUMBER Critical Infrastructure Protection (CIP), Project Code 125				
COST ($ in Millions)	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	Cost to Complete	Total Cost
Critical Infrastructure Protection Project 125	19.166	13.643	12.667	12.731	13.014	13.162	13.367	13.573	Continues	Continues

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 the availability of networked assets critical to DoD missions, to include DoD and non-DoD, domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining United States military operations on a global basis. Through identifying Defense Critical Assets, assessing them to determine vulnerabilities, incorporating specific threat and hazard information and analysis, and visually displaying relevant infrastructure data and analysis, DoD will be positioned to make risk management decisions to ensure the appropriate infrastructure is available, when needed, to support DoD missions.

Specifically, Combatant Commands (COCOMs) are responsible for identifying the mission capability requirements and coordinating with the Military Departments, Defense Agencies, DoD Field Activities, and Defense Sector Lead Agents to identify and assess Defense Critical Assets. As asset owners and capability providers, the Secretaries of the Military Departments and the Directors of Defense Agencies and DoD Field Activities, coordinate with the COCOMs to identify and prioritize the assets required to support mission-essential functions. Asset owners will also assess identified Defense Critical Assets to identify vulnerabilities and apply appropriate remediation and mitigation measures. 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.

Each Defense Sector Lead Agent, as identified in DoDD3020.40.DoD, represents one of ten (10) functional areas that provide support to the Combatant Commanders and asset owners. 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 2007

B. Program Change Summary

	FY 2006	FY 2007	FY 2008	FY 2009
Accomplishment/Subtotal Cost	10.778	2.956	1.542	1.500

DCIP Strategic Partnerships and Enabling Technologies

FY 2006: The program has:

- Institutionalized an inter-agency process to identify authoritative geospatial data sources for use across the DoD, the Federal interagency, and, state and local governments.
- Developed Knowledge Display and Aggregation System (KDAS) initial operating capability, leveraging the National Geospatial Intelligence Agency's (NGA) Palanterra system.
- Established web-services for 5 Defense Sector databases with KDAS/Palanterra for visualization of defense sector assets to provide situational awareness to senior leaders for strategic decision making.
- Published the DCIP Geospatial Data Strategy for the creation and maintenance of a common and comprehensive foundation of homeland infrastructure geospatial data. This effort ensures consistency of information used for display, analysis, and presentation of critical infrastructure in a Common Operational Picture (COP) environment.
- Initiated Independent Verification and Validation of Defense databases and tools suites used to conduct defense and commercial interdependency analysis.
- Developed scenario based, interactive exercise simulations to supplement existing table top, command post, and full scale incident response training and exercise programs.
- Determined emergency remediation infrastructure options for post-disaster reconstitution efforts

FY2007: The program will:

- Establish web services for remaining Defense Sector databases, Combatant Command, and Military Service

databases for visualization of assets in KDAS/Palanterra visualization tool to create a DCIP COP.
- Ingest information from National Labs on consequence assessment and predictive analysis tool suites to support pre-planning and positioning of defense assets.
- Develop capabilities to identify and provide risk management for critical infrastructure system vulnerabilities as a result of cyber based attacks

FY 2008: 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 Defense Industrial Base (DIB) assets.
- Develop protocols and standards to ensure interoperability of Homeland Security Information Network Components and DCIP COP for a HLS/HLD COP and situational awareness.

FY 2009: 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 Defense Industrial Base (DIB) assets.

Exhibit R-2a, RDT&E Project Justification	Date: February 2007

	FY 2006	FY 2007	FY 2008	FY 2009
Accomplishment/Subtotal Cost	8.388	10.687	11.125	11.231

DCIP Plans, Programs, and Capabilities Integrated and Implemented at All Levels

FY 2006: The program has:
- Published supporting foundation infrastructure standards and benchmarks for use by assessment programs across the Department of Defense and Defense Industrial Base (DIB) complex.
- Developed, in collaboration with the National Guard Bureau, WV National Guard , US Joint Forces Command and US Army TRADOC, DoD DCIP assessment training curriculum to support incorporation of infrastructure assessment standards and benchmarks into existing assessment programs.

- Published a DCIP Interim Implementation Guidance (IIG) as a bridging document to formal coordination and issuance of a DCIP DoD Instruction (DoDI). The IIG provides detailed implementation guidance, standards, lexicons, definitions for use by Combatant Commanders, Services, and Defense Agencies.
- Established an Integrated Product Team (IPT) to work issues related to drafting and publishing a DCIP DoDI
- Drafted a Department of Defense criticality methodology to identify defense critical assets
- Conducted functional mission decomposition of the Net-Centric Operations and Civil Support Joint Capability Areas (JCAs)
- 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., as well as participated in DoD led exercises.

FY2007: The program will:

- Coordinate and publish a DCIP DoD Instruction (DoDI), leveraging the DCIP DoDI IPT, and previously published IIG and lessons learned as the baseline
- Incorporate DoD DCIP assessment training curriculum into established DoD education and training programs
- Coordinate and publish the DoD criticality methodology to identify defense critical assets
- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical assets contained on the COCOM Integrated Priority List (IPL)
- Publish the DCIP Risk Assessment Handbook (which features the DCIP Characterization Process, Dependency Analysis Process, Criticality Process, Assessment Process, Threat/Hazard Process, Monitor & Reporting Process and the Risk Analysis Process)
- 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., as well as participated in DoD led exercises.

FY 2008: The program will:

- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical assets contained on the COCOM Integrated Priority List (IPL)
- Apply risk management methodology to all identified critical assets
- Develop a prioritization methodology to substantiate investment in risk management recommendations
- Perform trend analysis and develop remediation and mitigation options for addressing risks identified as part of the assessment process.
- Develop a prioritization methodology to substantiate investment in risk management recommendations

- Provide technical analysis and recommendations on infrastructure networks, points of service, interdependencies, and priority restoration for pre-event and post-event analysis for manmade or natural disaster incidents, and intelligence relating to possible terrorist threats.

FY 2009: The program will:

- Provide technical analysis and recommendations on infrastructure networks, points of service, interdependencies, and priority restoration for pre-event and post-event analysis for manmade or natural disaster incidents, and intelligence relating to possible terrorist threats.
- Conduct and maintain commercial infrastructure intra- and inter-dependency analysis on a minimum of 20 DoD critical assets contained on the COCOM Integrated Priority List (IPL)
- Apply risk management methodology to all identified critical assets
- Perform trend analysis and develop remediation and mitigation options for addressing risks identified as part of the assessment process.

C. Other Program Funding Summary: DCIP O&M funding is allocated to the Military Services, the Defense Sectors/Defense Agencies, and to OSD DCIP as the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). O&M 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 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
O&M,DW 0902198D8Z	29.579	20.567	18.997	20.053	20.322	19.829	20.233	20.635

D. Acquisition Strategy: N/A

E. Major Performers: N/A