Exhibit R-2, RDT&E Budget Item Justification						Date: February 2005		
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7				R-1 Item Nomenclature: Information Systems Security Program PE 0303140D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	21.349	10.495	12.546	12.853	13.471	13.618	13.752	14.354

A. Mission Description and Budget Item Justification:

The NII Information Systems Security Program (ISSP) provides focused research, development, testing and integration of technology and technical solutions critical to the Defense Information Assurance Program (10 USC 2224) through pilot programs and technology demonstration; investment in high leverage, near-term programs that offer immediate Information Assurance (IA) benefit; federal and multi-national initiatives; and short-term studies and research critical to protecting and defending information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These efforts focus on Computer Network Defense (CND) and the restoration of information systems by incorporating protection, detection, analysis and reaction and response capabilities; emerging cryptographic technologies; technology transition and IA research capabilities. This program is designed to meet the requirements of 10 USC 2224 (Defense Information Assurance Program), 44 USC 3544, (Federal Information Security Management Act of 2002), OMB Circular A-130, and DoD Directives 8500.1, and 0-8530.1. This program is funded under Budget activity 7, Operational System Development because it integrates technology and technical solutions to the Defense Information Assurance Program.

FY 2004 Accomplishments ($21.349 million):

- Conducted a feasibility study of modifying the existing Malta entity extraction server to work with Arabic text. Obtained a license and training for the current Malta server so that researchers in knowledge engineering could evaluate the Malta server technology for applicability to a broader scope of entity extraction needs.

- The Network Information and Space Security Center (NISSC) provides research, education, training, and other support to aid in mission accomplishments within military and civilian agencies. In 2004 the NISSC partnered with Universities and Industry to support research projects in homeland security and homeland defense. These research projects focused on the following areas: homeland security/homeland defense information sharing, fusion of intelligence data across national borders and federal/state/local entities, space systems to support homeland security and homeland defense, technical policy issues in moving from “need-to-know” to “need-to-share” environment, assessment and protection of critical infrastructures and their support systems, assessment of transnational health threats, and cyber-security threats in the new world of terrorism and prevention/detection/response mechanisms. This

research has provided military and civilian agencies with courses, academic programs, training programs, and research documentation that have increased their knowledge and awareness of the issues homeland security/homeland defense face in the future.

- Launched the Trusted Communications Study, an effort to address all Information Assurance (IA) concerns in a single chip. This project addressed the possibility of influencing the insertion of Government security features in commercial chip design. This task enabled the Government to have indirect input into commercial chip design, which will increase the security capabilities of chips that are being developed for use commercially and by the Government.

- Procured and implemented software capability and security enhancements in the QSec 2700 Secure Code Division Multiple Access (CDMA) Cell Phones that include the eight following programmable dePAC parameters: United States, United Kingdom, Australia, New Zealand, Canada, Combined Communications Electronics board Nations, North Atlantic Treaty Organization, and United States Coalition Partners; and the implementation of Enhanced Firefly.

- Developed and piloted an automated security certification and accreditation (C&A) process for DoD information systems (Digital DITSCAP). Began expansion into a more robust web services-based design called the Enterprise Mission Assurance Support System (eMASS) using shared information and services to deliver improved functionality over all the core IA processes by interconnecting all data transactions via a common database. Completed the first module of eMASS (June 04), authored baseline DoD IA controls implementation and validation materials, and initiated development of web-services based C&A and Vulnerability Management modules. Initiated a second pilot to baseline eMASS-enabled business process improvements and deployment aids.

- Developed IA architecture, policy and identified IA capabilities necessary to support and “end-to-end” IA capability for the GIG – including Transformational Communications, GIG Bandwidth Expansion, JTRS, and GIG Enterprise Services (GES)/Net Centric Enterprise Service (NCES) capabilities such as discovery, collaboration, messaging, mediation, data tagging, etc.

- Initiated a major Software Assurance study to develop processes and structures to mitigate the risks of malicious code and other threats introduced into information technology products (from foreign intelligence sources, other adversaries and competitors influencing, infiltrating and becoming technology vendors of information technology products and services (both foreign or domestic) or from intentional or unintentional changes to software by individuals)

- Developed information assurance techniques/processes for allied and coalition operations, including continued research and testing with Combined Communications Electronics Board (CCEB) with Australia, Canada, New Zealand and the U.K., the Multinational Interoperability Council (MIC) with Australia, Canada, France, Germany and U.K., and with the international test bed at the Joint Battle Center. Develop alternative network design and security concepts for improved coalition operations, including using PKI-Enabled Extended Markup Language (XML) for Cross-Security Domain Information Exchange and developing initial technical requirements specification for a "collaboration and browse" cross-domain solution.

- Developed a Commercial Innovation Integration (CII) process to better leverage commercial research activities (e.g., Venture Capital) for DoD Information Assurance, resulting in over 13 new partnerships using new technologies, practice, or processes for information assurance operations. Prepared initial study and proof of concept for a DoD Enterprise IA Portal.

- PKI and PKE. Explored design alternatives to current PKI tokens (PC and SmartCard) for the tactical and classified environment. Completed initial analysis of design and policy changes needed for multiple security domain tokens (one token for both unclassified/classified use). Continued support for the next stage of the Defense Cross-credentialing Information System (DCIS) pilot, which is focused on identifying and resolving interoperability issues between the electronic credentials of the Defense Department and its commercial partners.

- Supported research into new and enhanced attribution and trace back tools on enterprise level (local enclave through Service CERT to DoD CERT/JTF-CNO). Developed design requirements for improved auditing capabilities to identify, alert and analyze anomalous insider activities, with pilot projects underway for both Operating System (OS) "wrappers" (detecting unauthorized changes to OS) and anomaly detection with DISA and USMC.

- Researched and analyze enhanced Computer Network Defense (CND), vulnerability management and situational awareness tools that can be used and integrated throughout the DoD enterprise. Evaluation on vulnerability management scanning tool and DoD Enterprise-wide license for scanning tool awarded. Evaluation of vulnerability "patching" tool and OS wrappers.

- Continued development of CND Architecture initiated requirements development for the DoD CND Enterprise Sensor Grid and User Defined Operational Picture (both essential to provide IA and CND command and controls and situational awareness).

- Completed first IA assessment in preparation of establishing and IA and CND metrics program.

FY 2005 Plans ($10.495 million):

- Continue development of eMASS into a deployed enterprise information assurance management service. Baseline all DoD and IC IA policies and guidelines, and develop a mapping and translation service for jointly accredited information systems. Work with other federal agencies, e.g., NIST or DHS, to baseline and map to other federal IA policies and guidelines. Develop a capability to map IA policies and architectures to IA metrics and reporting requirements (e.g., FISMA). Continue modular development and deployment of additional services to support core IA processes, e.g., investment and resource management, workforce management, ports and protocols management.

- Continue development of IA architecture, policy and identify IA capabilities necessary to support and "end-to-end" IA capability for the GIG – including Transformational Communications, GIG Bandwidth Expansion, JTRS, and GIG Enterprise Services (GES)/NetCentric Enterprise Service (NCES) capabilities such as discovery, collaboration, messaging, mediation, data tagging, etc. Pilot the initial capability to integrate CND Architecture designs with the GIG IA Architecture development and the design of the Enterprise Sensor Grid.

- Continue development of the Commercial Innovation Integration (CII) process to leverage commercial research activities for DoD Information Assurance. Field prototype IA Portal.

- Complete the Software Assurance study and begin implementation of recommendations.

- Insider Threat - CND/Information Assurance/Information Operations Attribution Capability Initiative. Leveraging work done in FY 2003 and FY 2004, prototype and test enterprise attribution and trace back tools. Demonstrate interoperable software solution across a joint Inter-Service/Agency networked environment to quickly and effectively identify anomalous network activities with centralized visibility and control at the JTF-GNO level; pilot & Assess tools within the JTF-GNO and JFCOM to facilitate the ability to attribute hostile action in cyber-space to the person or people involved - pilot efforts will assess the capabilities that can rapidly and legally attribute an attack to an attacker (traceback), and do so across multiple, disparate network technologies and infrastructures, including wireless networks; pilot and assess tools and techniques within the JTF-GNO and JFCOM that are effective at reconstructing cyber event histories.

- Develop and prototype enterprise CND, vulnerability management and situational awareness tools identified in FY 2003/FY 2004. Integrate output of network scanner results into Enterprise Sensor Grid (ESG) and Situational Awareness/UDOP Databases to facilitate development of ESG engineering solutions; develop initial integrated view and pilot of sensor outputs for user level control at the JTF-GNO; enhance NSA developed prototype passive network mapping product and pilot within the JTF-GNO; develop a "Federation of Sensors" across a Joint Inter-Service/Agency implementation with sensor outputs integrated into a central console for centralized intrusion detection and warning; integrate/develop interoperability between IA Vulnerability Management VMS DB and the DoD Ports & Protocols DB and NIPRNet/CAP DB's to provide integrated view of system and component vulnerabilities across the DoD Networks

- Design and test prototype networks to improve information assurance and information sharing on coalition networks (CCEB, MIC, etc.); develop design criteria for improved "guards" for connection between differing security domains; selected prototype development of high priority guarding solutions; support technology demonstrations of secure metadata tagging and cross-security domain transfer using metadata tags

FY 2006 Plans ($12.546 million):

- Complete development of eMASS into a deployed enterprise information assurance management tool and provide as piloted IA Core Enterprise Service.

- Continue refinement of IA architecture, policy and IA capabilities necessary to support and "end-to-end" IA capability for the GIG – including enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Support technology demonstration, development and pilots.

- Leveraging work done in FY 2004/2005, continue experimentation, technology demonstration, prototype and test attribution, anomaly detection, trace-back, CND response action tools, with emphasis on DoD enterprise level application.

- Continue the testing, evaluation and focused piloting of various enterprise CND, vulnerability management and situational awareness tools as they evolve in capability.

- Continue technology demonstrations, piloting and selected research into cross-domain technologies to support information sharing between allies and coalition partners, concentrating on exploring on support of emerging

protocols and services and solutions utilizing metadata tagging.

FY 2007 Plans: ($12.853 million)

- Convert eMASS into a Core Enterprise Service information assurance management tool.

- Continue refinement of IA architecture, policy and IA capabilities necessary to support and "end-to-end" IA capability for the GIG – including enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Support technology demonstration, development and pilots focusing functions required in mid-term (2009-2012) increment of the IA Component of the GIG Architecture.

- Continue experimentation, technology demonstration, prototype and test evolving CND/situational awareness, vulnerability management, attribution, anomaly detection, trace back and response tools.

B. **Program Change Summary:** (Show total funding, schedule, and technical changes for the program element that have occurred since the previous President's Budget Submission)

	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget	14.576	11.135	12.201	12.515
Current President's Budget	21.349	10.495	12.546	12.853
Total Adjustments	6.773	-0.640	0.345	0.338
Congressional program reductions				
Congressional rescissions, Inflation adjustments		-0.640	0.345	0.338
Congressional increases				
SBIR/STTR Transfer				
Reprogrammings	6.773			

Change Summary Explanation:
FY 2004: Reprogramming from NSA 6.773 million
FY 2005: IT reduction -0.380 million; Management Improvement -0.034 million; General Reduction -0.068 million; FFRDC -0.049 million; CAAS -0.109 million
FY 2006: Non-Pay Purchase 0.394 million; Contract Support -0.049 million
FY 2007: Non-Pay Purchase 0.392 million; Contract Support -0.054 million

C. **Other Program Funding Summary**:

	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Total Cost
O&M, DW (PE0902198D8Z)	16.745	20.681	17.882	18.168	18.220	18.594	18.887	19.403	148.58

D. **Acquisition Strategy**: N/A

E. **Performance Metrics**:

- eMASS fielded and provides data support for FISMA;
- eMASS available as a Core Enterprise Service capability;
- IA Architecture incorporated into supported program plans;
- CND Architecture incorporated into IA Architecture;
- IA Portal prototype fielded and used by DoD IA Community;
- Pilots/technology demonstrations effect IA product development, concepts of operations development, or enterprise license decisions;
- Enterprise licenses for vulnerability patching and operating system wrappers awarded;
- DoD sensors integrated into an Enterprise Sensor Grid;
- Secure data tagging technology advanced;
- CND Response Action tools tested.

Exhibit R-2, RDT&E Budget Item Justification									Date: February 2005	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense Wide (0400), Budget Activity 7				R-1 ITEM NOMENCLATURE 0305125D8Z/CRITICAL INFRASTRUCTURE PROTECTION (CIP)						
COST ($ in Millions)	FY 2004*	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Cost to Complete	Total Cost
Total PE Cost	6.156	27.367	11.363	12.229	12.873	12.851	13.056	13.300	Continues	Continues
Critical Infrastructure Protection Project 125	6.156	27.367	11.363	12.229	12.873	12.851	13.056	13.300	Continues	Continues

A. Mission Description and Budget Item Justification

Homeland Security Presidential Directive #7 (HSPD-7) 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 protection 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 vulnerabilities. Risk is managed by balancing probability of threat, impact of loss, and extent of the vulnerability. 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.

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2005

B. Program Change Summary: Funding promoted 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. Funding identified, prioritized, and managed the risk associated with critical assets supporting DoD mission objectives both at home and in forward deployed areas.

COST ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget	2.023	27.021	11.108	11.952
Current BES/President's Budget	6.156	27.367	11.363	12.229
Total Adjustments:				
Congressional program reductions				
Congressional rescissions				
Congressional increases				
Reprogrammings				
SBIR/SSTR Transfer				
Program Adjustment	4.133	0.346	0.255	0.277

C. Other Program Funding Summary:

COST ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
RDT&E,N 0603235N	12.2							
RDT&E,N 0603734N	13.2							
O&M,DW D8Z	25.9	10.7	23.3	23.1	11.9	12.0	12.4	12.7

D. Acquisition Strategy: N/A

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2005

E. Performance Metrics:

FY 2005 Performance Metrics

- Conduct up to 12 Critical Infrastructure Protection pilot assessments in coordination with the Joint Staff's Joint Staff Integrated Vulnerability Assessments
- Identify vulnerabilities from completed assessments and perform trend analysis for mitigation recommendations
- Prototype a DCIP Enterprise Architecture

FY 2006 – FY 2011 Performance Metrics

- Establish Full Spectrum Integrated Vulnerability Assessment standards from the results of Critical Infrastructure Protection pilot assessment
- Implement a Defense Critical Infrastructure Protection Enterprise Architecture
- Develop a prioritization methodology to substantiate investment in mitigation recommendations
- Identify vulnerabilities from completed assessments and perform trend analysis for mitigation recommendations

Exhibit R-2a, RDT&E Project Justification									Date: February 2005	
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense Wide (0400), BA 7			PROGRAM ELEMENT 0305125D8Z			PROJECT NAME AND NUMBER CRITICAL INFRASTRUCTURE PROTECTION (CIP)				
COST ($ in Millions)	FY 2004*	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Cost to Complete	Total Cost
Critical Infrastructure Protection Project 125	6.156	27.367	11.363	12.229	12.873	12.851	13.056	13.300	Continues	Continues

* Previous funding in the Navy RDT&E.

A. Mission Description and Budget Item Justification:

The Defense Critical Infrastructure Program seeks to ensure that defense critical infrastructure, which includes DoD and non-DoD, domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis, shall be available when required. Vulnerabilities identified in defense critical infrastructure through this effort are prioritized for remediation or mitigation by responsible DoD authorities.

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.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	4.133	13.250	7.811	8.517

Understanding Risks Through Analysis And Assessment:

FY2004: The program developed and maintained the capability to ensure that a designated Mission Assurance Support Center (MASC), formerly known as the Mission Assurance Operations Center, was staffed and equipped for receipt of operational taskings, action tracking of critical infrastructure workload, and information exchanges. Responded to Mission Assurance (MA) related information requests on a timely, effective basis. This requirement supported the ability to obtain quick response, accurate infrastructure analysis, assessment, status, and critical infrastructure relationships to emerging threat information. Identified, prioritized, and managed risk assets associated with critical infrastructure supporting DoD missions.

Exhibit R-2a, RDT&E Project Justification	Date: February 2005

FY2005: The program will:

- Identify the 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) infrastructure areas: energy (electric power, natural gas); chemicals; transportation; telecommunications; water; and petroleum, oil, lubricants (POL).
- Develop and implement a Concept of Operations, standards, and modules for a Full Spectrum Integrated Vulnerability Assessment (FSIVA). Develop comprehensive training material, to include accreditation and certification criteria for assessment team personnel. FSIVA teams, conduct 12 pilot assessments on identified and prioritized critical assets to quantify vulnerabilities and associated risks and validate FSIVA methodology.
- 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.
- Perform vulnerability trend analysis and develop remediation and mitigation options for addressing vulnerabilities based on associated risks identified as part of the assessment process.

FY 2006: The program will:

- Implement improvements to the methodology for identifying critical assets.
- Conduct FSIVAs on critical assets identified through the modified analysis and assessment process implemented in FY 2005.
- Maintain critical assets and supporting data in the DCIP Data Management System (DMS) as the integrated repository for all mission analysis and characterization data.
- Develop, leverage, maintain, and enhance tools and data sets based on the requirements derived from the DCIP community and the output of FY 2005 pilot efforts.
- Support program office taskings for designated on-site assessments, designated National Special Security Events, validated requests from Combatant Commands, and other quick-response taskings

Exhibit R-2a, RDT&E Project Justification	Date: February 2005

FY 2007: The program will:

- Review requirements from the Combatant Commands, Military Services, and Defense Sectors and make adjustments to the methodology for identifying critical assets through Combatant Command mission analysis, Military Service characterization, Defense Sector characterization, and foundational infrastructure characterization.
- Promulgate this capability and methodology across DoD.
- Adjust tools and data sets based on solicited requirements to support analysis and characterization.
- Maintain the integrated repository for all mission analysis and characterization data in the DCIP DMS.
- Support program office taskings for designated on-site assessments, designated National Special Security Events, validated requests from Combatant Commands, and other quick-response taskings

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	0	3.624	.776	0

Prepare, Plan, And Respond To Incidents:

FY2005: The program will:

- Develop the Homeland Defense Mission Assurance Portal (HD-MAP) and the DCIP Data Management System (DMS) by including additional data sources and user-validated capabilities and integrating these enhancements into the DCIP Enterprise Architecture (EA).
- Use HD-MAP to support DoD in addressing its responsibilities to identify, prioritize and protect our most critical defense assets, foundation infrastructure assets and the defense industrial base.
- Provide a centralized point of access for Combatant Commanders and the services to obtain mission impact information to enable rapid response to critical infrastructure-related terrorist and conflict events.
- 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 2005

FY 2006: The program will:

- Implement requirements for Homeland Defense Mission Assurance Portal (HD-MAP) collected, validated, and prioritized during FY 2005.
- Enhance the HD-MAP in accordance with the Defense Critical Infrastructure Protection community requirements to provide for the needs of the stakeholders.
- Review additional findings from both the Critical Infrastructure Protection pilot assessments and the analysis and characterization pilot effort for incorporation into the HD-MAP.
- Integrate data (assessment data, infrastructure data, etc.) supporting the Defense Critical Infrastructure Protection program into the HD-MAP.
- Provide liaisons to support information sharing and leveraging of Critical Infrastructure Protection related information and capabilities across the homeland security interagency community and coordinate with other government agencies.
- Continue to transition new and enhanced capabilities to the Mission Assurance Support Center.
- Provide a centralized point of access for Combatant Commanders and the services to obtain mission impact information to enable rapid response to critical infrastructure-related terrorist and conflict events.
- Provide an effective response capability to identify potential mission impacts to DoD from actual or anticipated events against U.S. or host nation infrastructure via analytic and assessment capabilities.

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	0	6.051	2.776	3.612

Provide Program Support And Integration:

FY 2005: The program will:

- Determine Education and Training requirements to ensure a cohesive DCIP effort and to accomplish program goals and objectives consistently across the community.
- Develop and institute a monitoring and reporting capability that will improve overall responsiveness to potential threatening situations associated with DCIP assets.

Exhibit R-2a, RDT&E Project Justification	Date: February 2005

- Develop and implement a responsive Research and Development and Technical Integration capability to evaluate the potential for new, technologies to provide added capability and value into the Defense Critical Infrastructure Protection Program. 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.
- Provide liaisons to coordinate with other government agencies to further information sharing and leveraging of Critical Infrastructure Protection information and capabilities across the interagency community.
- Provide a liaison focused on establishing cooperative agreements with the international community with related CIP interests relevant to those of the U.S. DOD.
- Develop 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 implementation 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 expertise, and support to the DCIP community.
- Complete documentation and pursue formal approval of the standardized DCIP methodology for conducting mission area analysis, foundational infrastructure analysis, and Defense Sector characterization.

FY 2006: The program will:

- Support and further the development and implementation of Defense Critical Infrastructure Protection (DCIP) foundational activities, including the finalization of the enterprise architecture operational view, technical view, and system furthering the implementation of a responsive research development capability to evaluate the integration of new technologies.
- Review, validate, prioritize, and develop new DCIP-related concepts. Areas of focus for concept development will be military mission assurance; commercial infrastructure remediation options; vulnerability assessment tools and methods; decision support systems; DCIP -focused operations centers; new techniques for mitigation, remediation, and response to infrastructure disruptions; and multi-level security systems for advanced information sharing.

Exhibit R-2a, RDT&E Project Justification	Date: February 2005

FY 2007: The program will:

- Implement Defense Critical Infrastructure Protection foundational activities, including enterprise architecture and responsive research development capabilities to evaluate the integration of new technologies.
- Evaluate and prioritize new DCIP-related concepts to be incorporated into the DCIP. Areas of focus for concept development will be military remediation options; commercial infrastructure mission assurance; vulnerability assessment tools and methods; decision support systems; Critical Infrastructure Protection -focused operations centers; new techniques for mitigation, remediation, and response to infrastructure disruptions; and multi-level security systems for advanced information sharing.

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/Subtotal Cost	2.023	4.442	0	0

Enable Management Initiatives:

FY 2004: Supports the Defense Program Office for Mission Assurance (DPO-MA)

- Developed modeling and simulation techniques to predict and track interdependencies of defense infrastructures and commercial infrastructures; assessed vulnerabilities of critical assets; recommended courses for mitigation of vulnerabilities; exchanged asset and criticality data; and combined these efforts and products into a standardized architecture for collaborative information exchange, monitoring, and reporting.

Exhibit R-2a, RDT&E Project Justification	Date: February 2005

FY2005: The program will:

- Recommend, draft, review, and revise documentation associated with mission assurance policy, strategy, and plans.
- Review, validate, and provide recommendations on requirements received from the Defense Critical Infrastructure Protection community.
- Perform a gap analysis of baseline capabilities and requirements against the DCIP core goals and objectives and provide results for future consideration and planning.
- 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.

B. Other Program Funding Summary: Funding provided to the Defense Program Office for Mission Assurance will support continued development of the capability to provide Combatant Commanders, military services and DoD mission planners with the ability to analyze their infrastructure dependencies and interdependencies and assess the potential impact on military operations as a result of disruptions to key infrastructure components.

COST ($ in Millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
RDT&E,N 0603235N	12.2							
RDT&E,N 0603734N	13.2							
O&M,DW 0902198D8Z	25.9	10.7	23.3	23.1	11.9	12.0	12.4	12.7

D. Acquisition Strategy: N/A

E. Major Performers: N/A

Exhibit R-2, RDT&E Budget Item Justification						Date: February 2005		
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7				R-1 Item Nomenclature: Defense Joint Counterintelligence Program PE 0305146D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	29.293	0	0	0	0	0	0	0
Horizontal Fusion	16.459	0	0	0	0	0	0	0
CI Data Conversion	12.834	0	0	0	0	0	0	0

A. Mission Description and Budget Item Justification:

DJCIP provides the ability to counter clandestine or covert threats to DoD personnel, operations, facilities, and to those DoD research/technology undertakings and critical infrastructures that the Department has determined to be among its highest priority concerns.

B. **Program Change Summary:** (Show total funding, schedule, and technical changes for the program element that have occurred since the previous President's Budget Submission)

	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget	30.312			
Current President's Budget	29.293			
Total Adjustments	-1.019			
Congressional program reductions				
Congressional rescissions				
Congressional increases				
Internal reprogramming	-1.019			
DERF Adds				

Change Summary Explanation:
FY 2005: Transferred to other program elements.

C. Other Program Funding Summary: Not Applicable

D. Acquisition Strategy: Not Applicable

E. Performance Metrics: Classified

Exhibit R-2a, RDT&E Project Justification							Date: February 2005	
Appropriation/Budget Activity RDT&E, Defense-Wide, BA 7				Project Name and Number: Horizontal Fusion/PE 0305146D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Name: Horizontal Fusion	16.459	0	0	0	0	0	0	0

A. Mission Description and Budget Item Justification:

The Secretary of Defense approved the establishment of the Horizontal Fusion Portfolio as one of his top ten priorities to make net-centric operations and warfighting a near-term operational reality consistent with the vision of force transformation. The Horizontal Fusion program overcomes acknowledged limitations in Joint Force operations caused by the inability to rapidly adjust plans and tactics for situational awareness while taking advantage of the explosion in battlefield intelligence and information sources such as advanced sensor equipped UAVs, improved Special Reconnaissance capabilities and ongoing developments and deployment of digitized support systems. Horizontal Fusion provides Joint Force Commanders and their Battle Staffs with needed capabilities for increasing the speed of Command of widely dispersed Joint Forces to operate against a wide range of threats and to support new methods of war fighting – emphasizing more rapid and effective integration of operational intelligence planning by providing operators on the edge with the applications and data access to effectively achieve situational awareness without latency and ensure that the entire chain of command can simultaneously view events as they unfold. The participants that make up the Horizontal Fusion portfolio are primarily existing programs of record, which require strict procurement and requirements control under traditional acquisition policy. The Horizontal Fusion portfolio maximizes these ongoing efforts by integrating existing capabilities and, therefore, leveraging the DoD's resources while accelerating their inclusion in the net-centric environment. The selection for participation in the HF portfolio is based on 1) highest priority programs for net-centric joint warfighting (to include coalition and allied efforts) 2) time and cost to implement, and 3) the Joint Forces Command matrix of required capabilities to meet near-term joint warfighting conops. Today, the US Army in Iraq is using tools developed as part of the Horizontal Fusion portfolio, such as the unattended ground sensor arrays. These acoustic sensors successfully locate mortars used to fire on US troops. These capabilities were demonstrated as part of the Army Research Lab's (ARL) Warrior's Edge project within the Horizontal Fusion Portfolio prior to being used in Iraq. Other HF operational capabilities, such as the acoustic sensor, are under development within the HF portfolio. Further, Horizontal Fusion provides for the practical net-centric implementation of interoperability required to achieve the Secretary's vision of transformation. It is a critical element in the successful implementation of the GIG systems architecture, Net-Centric Enterprise Services (NCES), DoD Data Management Strategy (DDMS) and the services oriented architecture for Information Assurance (IA). These programs support the idea of accelerating, "Revolutionary technologies that 'change minds' and ways of doing things.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/ Effort/Subtotal Cost	16.459	0	0	0
RDT&E Articles Quantity *(as applicable)				

FY 2004 Accomplishments: ($16.459)

- Demonstrated capability of Horizontal Fusion to be a force multiplier with Quantum Leap-1
- Continued efforts on first round of pilots
- Basic Language Translation (BLTS) is a web-enabled application to access language databases, provide immediate gist of paper documents to tactical forces, and posts document and translation to the net for in-depth analysis
- Global Net-Centric Surveillance and Targeting (GNSCT) uses smart software agents to find "possibles" in all available data; analyst does analysis vice combing databases
- Demonstrated capability of Horizontal Fusion in OEF and OIF with Quantum Leap-2
- Added new initiatives in second round of pilots
  - Pilot cross-domain information sharing, secure wireless, and additional infrastructure solutions
  - Increase opportunities for data providers and consumers to post and access data
- Selected focus areas for next round of pilots
  - Add new high-value data sources (working with IC to identify)
  - Expand secure wireless
  - Create secure, collaborative coalition environments
  - Use of situational awareness tools via high resolution VTC
  - Pilot command and control visualization

FY 2005 Accomplishments: N/A

FY 2006 Plans: N/A

FY 2007 Plans: N/A

C. Other Program Funding Summary:

	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Total Cost
O&M, DW (PE0902198D8Z)	2.800								2.800
Proc, DW (PE 0902199D8Z)	16.212								16.212
RDT&E, DW (0305190D8Z)	129.581								129.581

D. Acquisition Strategy. N/A

E. Major Performers: DIA, DISA, NGA, NSA, NRO, ARMY Research Laboratory, Army HQ/G2, Navy CEC program, SPAWAR System Center – Charleston, SPAWAR System Center – San Diego, Pennsylvania State University Applied Research Laboratory, John Hopkins University Applied Physics Laboratory, Patrick AFB, Ft. Benning, GA, SOCOM, PACOM, CENTCOM, USFK, Ft. Bragg, Ft. Belvoir, USMC Quantico, JFCOM, STRATCOM, NATO, NGIC, Naval Research Laboratory, Hanscom AFB, CECOM, Department of State, Office of Naval Research, Wright Patterson AFB, INSCOM

F. Performance Metrics: Performance is based on portfolio and initiative adherence to identified DoD net-centric attributes, support to speed of COCOM decision-making process, and measured support to cross-domain and coalition information sharing. Measures include:

- Number of programs of record that incorporate (1) Core Enterprise Services, (2) meta-tagging to locate, access and control access to data, and (3) net-centric information assurance.

- Number of programs of record that utilize the operational net-centric infrastructure (the collateral space) and other DoD CIO strategic investments.

- Number of Regional Support Centers (RSC's) and DoD Enterprise Computer Centers (DECC's) that have installed the operational baseline of net-centric capabilities provided by Horizontal Fusion.

- Number of programs of record that are able to share information with coalition partners and move to higher protection levels as identified by the DoD IA organization.

- A measured and shortened decision support cycle for COCOMs.

- A measured and shortened cycle for Time Critical Targeting.

- A measured and shortened cycle for analysts to correlate information for pattern recognition (both text and graphical) resulting in decreased timelines for event prediction and event influence.

- A measured and shortened cycle for communicating information and common blue/red force pictures during joint operations which include coalition and allied partners.

Exhibit R-2a, RDT&E Project Justification								Date: February 2005
Appropriation/Budget Activity RDT&E, Defense-Wide, BA 7				Project Name and Number: CI Data Conversion				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Name: CI Data Conversion	12.834	0	0	0	0	0	0	0

B. Mission Description and Budget Item Justification:

The Counterintelligence Field Activity (CIFA), as a component of the Office of the Under Secretary of Defense (Intelligence), has been tasked to support the protection of the Department of Defense (DoD) critical technologies from foreign intelligence service, terrorist, and other covert or clandestine threats. An important part of this task is the capture and conversion – including storing, analyzing, manipulating, and displaying – of massive amounts of current CI and technical data held by various DoD program offices and projects. Analysis conducted on the data, and comparison of effort across multiple programs, will help determine which case data or technologies are critical.

The desired effort is the capture and conversion of sensitive CI case, technical and design information combined with engineering and analytical support to the CIFA. A very large body of unclassified and classified CI case, technical, design, and engineering information resides in numerous DoD programs and projects. CIFA has an immediate need to capture and convert multiple terabytes of this unclassified and classified information and data. Additionally, much of this data is stored in disparate Databases.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/ Effort/Subtotal Cost	12.834	0	0	0
RDT&E Articles Quantity *(as applicable)				

FY 2004 Accomplishments: ($12.834)

- Expansion of CIFA Operating Capabilities
  - Developed plans to establish the Data Migration Center (DMC), to include manpower, roles and responsibilities, and analytical techniques

- Fielded the Rapid Deployment Conversion Suite (RDCS), to include IT and logistical information.

- Data Conversion, Transfer, and Storage
  - Provided the ability to transfer large amounts of data between the DMC and CIFA Facilities
  - Conversion of selected data holdings, to include Immigration and Naturalization Service data
  - Provided the RDCS for on-site scanning

FY 2005 Accomplishments: N/A

FY 2006 Plans: N/A

FY 2007 Plans: N/A

C. Other Program Funding Summary: N/A

D. Acquisition Strategy. N/A

E. Major Performers: Counterintelligence Field Activity (CIFA), Immigration and Natruralization Service (INS), AFOSI, NCIS, FCA, DSS, US Immigrations Law Enforcement Support Center

F. Performance Metrics: Performance is based on the increased data made available from this effort to the CI analyst and the ability to readily convert data.
Measures include:

- Percentage of data converted and transferred to CIFA from INS and other directed data sites
- Ability to deploy a capability to convert data on-site
- Effectiveness of on-site data conversion
- Quality of data converted both locally and on-site

Exhibit R-2, RDT&E Budget Item Justification					Date: February 2005			
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7					R-1 Item Nomenclature: C3I Intelligence Programs PE 0305190D8Z			
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	129.581							
Horizontal Fusion	123.018							
C3I Intelligence Program Support	4.600							
GWOT CENTRIX	1.963							

A. **Mission Description and Budget Item Justification**:
This program element supports intelligence activities focused on the development, integration and assessment of systems or applications in support of non-traditional and contingency warfare. Resources will also support network-centric collaborative operations to improve situational awareness and operational-intelligence planning efforts. This program is funded under BA-7, Operational Systems Development, because it supports intelligence efforts that involve engineering development.

FY 2004 Accomplishments: ($1.963 million)

GWOT - CENTRIX

- Supported development of multi-level thin client solution needed for ships and air operations centers.
- Implemented improved metadata tagging and search capabilities on coalition information sharing networks
- Provided for completion of CENTRIXS network interoperability certification.

B. Program Change Summary: (Show total funding, schedule, and technical changes for the program element that have occurred since the previous President's Budget Submission)

	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget	130.178			
Current BES/President's Budget	129.581			
Total Adjustments	-0.597			
Congressional program reductions				
Congressional rescissions, inflation adjustments	-0.597			
Congressional increases				
Reprogrammings				

Change Summary Explanation:
FY 2004: Non-Pay Inflation Adjustment -0.597

C. Other Program Funding Summary: N/A

D. Acquisition Strategy: N/A

Exhibit R-2a, RDT&E Project Justification							Date: February 2005	
Appropriation/Budget Activity RDT&E, Defense-Wide, BA 7				Project Name and Number: Horizontal Fusion/0305190D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Name: Horizontal Fusion	123.018							
GWOT - Horizontal Fusion	4.600							

A. Mission Description and Budget Item Justification:

The Secretary of Defense approved the establishment of the Horizontal Fusion Portfolio as one of his top ten priorities to make net-centric operations and warfighting a near-term operational reality consistent with the vision of force transformation. The Horizontal Fusion program overcomes acknowledged limitations in Joint Force operations caused by the inability to rapidly adjust plans and tactics for situational awareness while taking advantage of the explosion in battlefield intelligence and information sources such as advanced sensor equipped UAVs, improved Special Reconnaissance capabilities and ongoing developments and deployment of digitized support systems. Horizontal Fusion provides Joint Force Commanders and their Battle Staffs with needed capabilities for increasing the speed of Command of widely dispersed Joint Forces to operate against a wide range of threats and to support new methods of war fighting – emphasizing more rapid and effective integration of operational intelligence planning by providing operators on the edge with the applications and data access to effectively achieve situational awareness without latency and ensure that the entire chain of command can simultaneously view events as they unfold. The participants that make up the Horizontal Fusion portfolio are primarily existing programs of record, which require strict procurement and requirements control under traditional acquisition policy. The Horizontal Fusion portfolio maximizes these ongoing efforts by integrating existing capabilities and, therefore, leveraging the DoD's resources while accelerating their inclusion in the net-centric environment. The selection for participation in the HF portfolio is based on 1) highest priority programs for net-centric joint warfighting (to include coalition and allied efforts) 2) time and cost to implement, and 3) the Joint Forces Command matrix of required capabilities to meet near-term joint warfighting conops. Today, the US Army in Iraq is using tools developed as part of the Horizontal Fusion portfolio, such as the unattended ground sensor arrays. These acoustic sensors successfully locate mortars used to fire on US troops. These capabilities were demonstrated as part of the Army Research Lab's (ARL) Warrior's Edge project within the Horizontal Fusion Portfolio prior to being used in Iraq. Other HF operational capabilities, such as the acoustic sensor, are under development within the HF portfolio. Further, Horizontal Fusion provides for the practical net-centric implementation of interoperability required to achieve the Secretary's vision of transformation. It is a critical element in the successful implementation of the GIG systems architecture, Net-Centric Enterprise Services (NCES), DoD Data Management Strategy (DDMS) and the services oriented architecture for Information Assurance (IA). These programs support the idea of accelerating, "Revolutionary technologies that 'change minds' and ways of doing things.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/ Effort/Subtotal Cost	127.618			
RDT&E Articles Quantity *(as applicable)				

FY 2004 Accomplishments: ($127.618)

- Demonstrated capability of Horizontal Fusion to be a force multiplier with Quantum Leap-1
- Continued efforts on first round of pilots
- Basic Language Translation (BLTS) is a web-enabled application to access language databases, provide immediate gist of paper documents to tactical forces, and posts document and translation to the net for in-depth analysis
- Global Net-Centric Surveillance and Targeting (GNSCT) uses smart software agents to find "possibles" in all available data; analyst does analysis vice combing databases
- Demonstrated capability of Horizontal Fusion in OEF and OIF with Quantum Leap-2
- Added new initiatives in second round of pilots
  - Pilot cross-domain information sharing, secure wireless, and additional infrastructure solutions
  - Increase opportunities for data providers and consumers to post and access data
- Selected focus areas for next round of pilots
  - Add new high-value data sources (working with IC to identify)
  - Expand secure wireless
  - Create secure, collaborative coalition environments
  - Use of situational awareness tools via high resolution VTC
  - Pilot command and control visualization

FY 2005 Plans: N/A

FY 2006 Plans: N/A

FY 2007 Plans: N/A

C. Other Program Funding Summary:

	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Total Cost
O&M, DW (PE0902198D8Z)	2.800								2.800
Proc, DW (PE 0902199D8Z)	6.212								6.212
RDT&E, DW (0305146D8Z)	16.565								16.565

Acquisition Strategy. **N/A**

E. Major Performers: DIA, DISA, NGA, NSA, NRO, ARMY Research Laboratory, Army HQ/G2, Navy CEC program, SPAWAR System Center – Charleston, SPAWAR System Center – San Diego, Pennsylvania State University Applied Research Laboratory, John Hopkins University Applied Physics Laboratory, Patrick AFB, Ft. Benning, GA, SOCOM, PACOM, CENTCOM, USFK, Ft. Bragg, Ft. Belvoir, USMC Quantico, JFCOM, STRATCOM, NATO, NGIC, Naval Research Laboratory, Hanscom AFB, CECOM, Department of State, Office of Naval Research, Wright Patterson AFB, INSCOM

F. Performance Metrics: Performance is based on portfolio and initiative adherence to identified DoD net-centric attributes, support to speed of COCOM decision-making process, and measured support to cross-domain and coalition information sharing. Measures include:

- Number of programs of record that incorporate (1) Core Enterprise Services, (2) meta-tagging to locate, access and control access to data, and (3) net-centric information assurance.

- Number of programs of record that utilize the operational net-centric infrastructure (the collateral space) and other DoD CIO strategic investments.

- Number of Regional Support Centers (RSC's) and DoD Enterprise Computer Centers (DECC's) that have installed the operational baseline of net-centric capabilities provided by Horizontal Fusion.

- Number of programs of record that are able to share information with coalition partners and move to higher protection levels as identified by the DoD IA organization.

- A measured and shortened decision support cycle for COCOMs.

- A measured and shortened cycle for Time Critical Targeting.

- A measured and shortened cycle for analysts to correlate information for pattern recognition (both text and graphical) resulting in decreased timelines for event prediction and event influence.

- A measured and shortened cycle for communicating information and common blue/red force pictures during joint operations which include coalition and allied partners.

Exhibit R-2, RDT&E Budget Item Justification							Date: February 2005	
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7				R-1 Item Nomenclature: Technology Development PE 0305191D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	244.411	0	0	0	0	0	0	0

A. Mission Description and Budget Item Justification:

Technology Development is a classified program. Program details are provided in the classified Congressional Justification Book. This program is funded under Budget Activity 7, Operational System Development because it supports intelligence efforts that involve engineering development.

FY 2004 Accomplishments:

- Mission Support $244.411

B. **Program Change Summary:** (Show total funding, schedule, and technical changes for the program element that have occurred since the previous President's Budget Submission)

	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget	245.536	0	0	0
Current President's Budget	244.411	0	0	0
Total Adjustments	-1.125			
Congressional program reductions				
Congressional rescissions				
Congressional increases				
Other Adjustments	-1.125			

Change Summary Explanation:

FY 2004: Miscellaneous reductions $1.125
FY 2005: Program transferred to Air Force.

C. Other Program Funding Summary: Not Applicable

D. Acquisition Strategy: Not Applicable

E. Performance Metrics: Classified

Exhibit R-2, RDT&E Budget Item Justification							Date February 2005	
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7				R-1 Item Nomenclature: Net Centricity PE 0305199D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	0.000	128.233	8.387	12.548	56.728	123.167	120.609	135.619
Horizontal Fusion		120.539	0.000	3.981	47.138	113.381	110.632	125.411
GIG Evaluation Facilities (GIG-EF) and GIG End-to-End Systems Engineering Advisory Activities		7.694	8.387	8.567	9.590	9.786	9.977	10.208

A. Mission Description and Budget Item Justification:

This program element will support information management and information technology activities focused on the development, integration, testing and assessment of capabilities and applications in support of joint and coalition warfighter needs. Resources will support net centric collaborative development and operations to improve situational awareness, interoperability and operational planning efforts. This program is funded under Budget Activity 7, Operational System Development, because it supports engineering development and testing of RDT&E activities.

The Horizontal Fusion Project funding in FY 2006 was realigned by the Department to support priority net centric transformation efforts such as information assurance, Multinational Information Sharing and Internet Protocol (IP) based capability into military communications satellites.

B. Program Change Summary: (Show total funding, schedule, and technical changes for the program element that have occurred since the previous President's Budget Submission)

	FY 2004	FY 2005	FY 2006	FY 2007
Previous President's Budget		214.222	103.924	125.620
Current President’s Budget		128.233	8.387	12.548
Total Adjustments		-85.989	-95.537	-113.072
Congressional program reductions				
Congressional rescissions, inflation adjustments		-5.989	0.229	0.328
Congressional increases				
Reprogrammings		-80.000	-85.766	-103.400
Transfer			-10.000	-10.000
Program Increase				

Program Change Summary Explanation:
FY 2005: Congressional Reprogramming to other Department efforts –80.000 million; IT reduction –2.911 million; Management Improvements -.406 million; General Reduction -.816 million; FFRDC Reduction -.583 million; CAAS reduction –1.273 million
FY 2006: Reprogrammed to other Department net centric efforts –85.766 million; transferred to Air Force for SAP activities –10.000 million; Non-pay Inflation Adjustments .263 million; Contracting Support -.034 million
FY 2007: Reprogrammed to other Department net centric efforts –103.400 million; transferred to Air Force for SAP activities –10.000 million; Non-pay Inflation Adjustment .382million; Contracting Support -.054 million

C. Other Program Funding Summary: N/A

D. Acquisition Strategy: N/A

Exhibit R-2a, RDT&E Project Justification							Date: February 2005	
Appropriation/Budget Activity RDT&E, Defense-Wide, BA 7				Project Name and Number: Horizontal Fusion/0305199D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Name: Horizontal Fusion		114.239	0.000	2.387	45.519	111.729	108.945	123.686
GWOT - Horizontal Fusion		6.300	0.000	1.594	1.619	1.652	1.687	1.725

A. Mission Description and Budget Item Justification:

The Secretary of Defense approved the establishment of the Horizontal Fusion Portfolio as one of his top ten priorities to make net-centric operations and warfighting a near-term operational reality consistent with the vision of force transformation. The Horizontal Fusion program also supports activities focused on the development, integration, testing and assessment of net centric capabilities, including those Information Assurance R&D activities necessary to implement the IA component of the GIG architecture essential to the transformation of the GIG. The participants that make up the Horizontal Fusion portfolio are primarily existing programs of record, which require strict procurement and requirements control under traditional acquisition policy. The Horizontal Fusion portfolio maximizes these ongoing efforts by integrating existing capabilities and, therefore, leveraging the DoD's resources while accelerating their inclusion in the net-centric environment. The selection for participation in the HF portfolio is based on 1) highest priority programs for net-centric joint warfighting (to include coalition and allied efforts) and GIG transformation on 2) time and cost to implement 3) the Joint Forces Command matrix of required capabilities to meet near-term joint warfighting conops and 4) the requirements of the IA component of the GIG architecture. Today, the US Army in Iraq is using tools developed as part of the Horizontal Fusion portfolio, such as the unattended ground sensor arrays. These acoustic sensors successfully locate mortars used to fire on US troops. These capabilities were demonstrated as part of the Army Research Lab's (ARL) Warrior's Edge project within the Horizontal Fusion Portfolio prior to being used in Iraq. Other HF operational capabilities, such as the acoustic sensor, are under development within the HF portfolio. Further, Horizontal Fusion provides for the practical net-centric implementation of interoperability and information assurance required to achieve the Secretary's vision of transformation. It is a critical element in the successful implementation of the GIG architecture (and its IA component), Net-Centric Enterprise Services (NCES), DoD Data Management Strategy (DDMS) and the services oriented architecture for Information Assurance (IA). These programs support the idea of accelerating, "Revolutionary technologies that 'change minds' and ways of doing things.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/ Effort/Subtotal Cost		120.539	0.000	3.981
RDT&E Articles Quantity *(as applicable)				

FY 2004 Accomplishments : N/A

FY 2005 Plans: ($120.539 million)

FY 2005 efforts will focus on implementation of net centric capabilities and processes directly to the warfighter and analysis of the operational baseline. As a result of funding constraints, no additional initiatives will be added to the horizontal fusion portfolio to further expand net centric capability. In addition, operational support to the existing portfolio will be curtailed.

- Transition HF demonstrated capabilities to operations by supporting the deployed forces of the XVIII ABC and OED community.
- Continue net-centric implementation of GIG architecture.
- Continue implementation and development of the IA component of the GIG architecture.
- Coordinate with Combatant commanders for their attaching to “the net.”
- Locate and incorporate additional operationally relevant information sources (both tactical and national for bi-lateral information sharing).
- Continue to refine the HF environment and services (i.e., Collaboration tool suite interoperability).
- Transition next generation of NCES pilot services to operational enterprise infrastructure.
- Leverage GIG Bandwidth expansion to refine information sharing and net-centric processes.
- Investigate and incorporate, as appropriate, multiple end users platforms (low end – palm computing to high-end desktops and servers).
- Continue to address streamlined security policy/certification and accreditation implementation with evaluation and testing of security technologies emphasizing cross-domain information exchange.
- Address tactics, techniques and procedures for net-centric operations within the Service schools and exercises.
- Continue to evaluate the parameters of the physical and logical edge of tactical data environments.

FY 2006 Plans: ($0 million)

N/A

FY 2007 Plans: ($3.981 million)

- Implement and develop the Information Assurance Component of the GIG Architecture.
- Develop standards, methods, and technologies to provide trusted identities and implement flexible and automated means to grant privileges on the network
- Conduct research in persistent monitoring, analysis and situational awareness insider and outside threats.

C. Other Program Funding Summary:

	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Total Cost
O&M, DW (PE0902198D8Z)	2.800	5.909	0.000	0.000	0.000	0.000	0.000	0.000	8.709
Proc, DW (PE 0902199D8Z)	6.212	10.102	0.000	0.000	0.000	0.000	0.000	0.000	16.314

D. Acquisition Strategy. N/A

E. Performance Metrics: Performance is based on portfolio and initiative adherence to identified DoD net-centric attributes, support to speed of COCOM decision-making process, and measured support to cross-domain and coalition information sharing. Measures include:

- Number of programs of record that incorporate (1) Core Enterprise Services, (2) meta-tagging to locate, access and control access to data, and (3) net-centric information assurance.

- Number of programs of record that utilize the operational net-centric infrastructure (the collateral space) and other DoD CIO strategic investments.

- Number of Regional Support Centers (RSC's) and DoD Enterprise Computer Centers (DECC's) that have installed the operational baseline of net-centric capabilities provided by Horizontal Fusion.

- Number of programs of record that are able to share information with coalition partners and move to higher protection levels as identified by the DoD IA organization.

- A measured and shortened decision support cycle for COCOMs.

- A measured and shortened cycle for Time Critical Targeting.

- A measured and shortened cycle for analysts to correlate information for pattern recognition (both text and graphical) resulting in decreased timelines for event prediction and event influence.

- A measured and shortened cycle for communicating information and common blue/red force pictures during joint operations, which include coalition and allied partners.

Exhibit R-2a, RDT&E Project Justification						Date: February 2005		
Appropriation/Budget Activity RDT&E, Defense-Wide, BA 7				Project Name and Number: GIG-EF/PE 0305199D8Z				
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Name: GIG Evaluation Facilities (GIG-EF) & GIG End-to-End SE Advisory Activities		7.694	8.387	8.567	9.590	9.786	9.977	10.208

A. Mission Description and Budget Item Justification:

The Global Information Grid (GIG) Evaluation Facilities and E2E Systems Engineering (SE) Advisory Activities project provides resources needed to test key systems in an end-to-end manner, including providing for system engineers, test-bed hardware, software and fiber optic connectivity at the Naval Research Laboratory and several other test locations in the U.S. The evaluation facilities will be used to demonstrate interoperability of multiple Transformational Communications programs including but not limited to the Joint Tactical Radio System (JTRS), Global Information Grid Bandwidth Expansion (GIG BE), Teleports, and Transformational Satellite Communications System (TSAT). For these systems GIG-EF & SE would:

-Perform tests that physically demonstrate technical performance.
-Provide an independent, overarching review of technology and interface standards.
-Ensure technical issues are identified early and schedules synchronized to produce a jointly interoperable, timely and cost-effective architecture development.
-Prevent costly program reworks and restructuring, and more importantly, avoid delays in providing joint warfighter connectivity.

The effort also provides engineering, integration and hardware and fiber optic connectivity necessary to validate the performance for key transformational communication programs. The funding will also provide the engineering resources necessary for performing the Global Information Grid (GIG) end-to-end systems engineering oversight function. Resources will be applied to end-to-end systems engineering topics related to the successful integration of several programs that will form the GIG in areas such as information assurance (IA), quality of service (QOS), network management, interface definition and standards selection, and routing protocols. These resources will work in conjunction with systems engineers from key GIG programs such as the Joint Tactical Radio System (JTRS), Transformational Satellite Communications System (TSAT), Teleport, GIG Bandwidth Expansion (GIG-BE), Warfighters Internet-Tactical (WIN-T), Net-Centric Enterprise Services (NCES) and Automated Digital Networking System (ADNS) to identify and address technical issues resulting from engineering decisions made without the end-to-end perspective.

B. Accomplishments/Planned Program

	FY 2004	FY 2005	FY 2006	FY 2007
Accomplishment/ Effort/Subtotal Cost		7.694	8.387	8.567
RDT&E Articles Quantity *(as applicable)				

FY 2004 Accomplishments: N/A

FY 2005 Plans: ($7.694 million)

- Develop the first increment of the GIG end to end quality of service framework
- Work with NSA to complete the GIG IA architecture
- Develop the first increment of the end to end GIG routing architecture
- Review WIN-T, ADNS, JTRS Cluster One, and GIG-BE for compliance to end to end GIG frameworks, architectures, and design guidance
- Work with systems engineering organizations from GIG programs to identify and address cross-program issues and influence programs to implement compatible designs that maximize end to end performance
- Establish GIG-EF capabilities providing interoperability and connectivity to support OC-192 (10 Gb) end-to-end testing among key GIG transport program activities and OC-48 connectivity to Service (WIN-T, FORCENET, MC2, etc.), Combatant Command (JFCOM, STRATCOM, etc.) and other GIG activities (JTRS, Teleport, etc.) to ensure programs meet GIG architectural requirements.
- Develop and maintain a testing suite capable of supporting passive and active IP monitoring and injection of GIG-like traffic and hostile attacks
- Perform end-to-end testing and experimentation in support of GIG developer requirements including but not limited to:
    - JTRS Wideband Networking Waveform early testing (Cluster 2)
    - High Assurance IP Encryption (HAIPE) 1-10 Gb Terrestrial
    - Support warfighting interoperability experimentation via the Joint Rapid Architecture Experimentation (JRAE) and US Joint Forces Command (USJFCOM) Joint Battle Management C2 (JBMC2) Activity including Quality of Service, efficient routing and scalability
    - DoD IPv6 Transition (pilot programs)
    - Joint C2, applications and platform testing activities such as JITC

FY 2006 Plans: ($8.387 million)

- Develop the second increment of the GIG end to end quality of service framework
- Work with NSA to complete the GIG IA architecture
- Develop the second increment of the end to end GIG routing architecture
- Complete the end to end GIG network management framework
- Review E-10A, JTRS Cluster Five, FAB-T, WGS, and Teleport for compliance to end to end GIG frameworks, architectures, and design guidance
- Work with systems engineering organizations from GIG programs to identify and address cross-program issues and influence programs to implement compatible designs that maximize end to end performance
- Continued support of GIG-EF capabilities and enhancements via connectivity to Allied and Coalition activities and operational networks.
- Perform end-to-end testing and experimentation in support of GIG developer requirements including but not limited to:
    - JTRS WNW (Cluster 5 and early Cluster 1)
    - HAIPE 10 Gb implementation
    - HAIPE 10 Gb Optical Encryptors early testing
    - Netcentric Core Enterprise Services early testing
    - DoD IPv6 experimentation and transition
    - Support warfighter interoperability experimentation via JRAE tests in coordination with USJFCOM JBMC2 activities
    - Joint C2, applications and platform testing activities such as JITC

FY 2007 Plans: ($8.567 million)

- Ensure the GIG end to end quality of service framework evolves in accordance with the evolution of commercial products, services, and technology
- Refine the GIG IA, routing architecture, and network management framework to be consistent with evolving commercial products, services, and technology

- Review JTRS Cluster AMF, TSAT, JC2, and NCES for compliance to end to end GIG frameworks, architectures, and design guidance
- Work with systems engineering organizations from GIG programs to identify and address cross-program issues and influence programs to implement compatible designs that maximize end to end performance
- Analyze end to end systems engineering issues by review technical documentation, working with the systems engineering organizations of each of the programs, employing modeling and simulation, and using the results of end to end systems engineering testing and influence design changes to programs to assure compatibility and to maximize end to end performance
- Continued support of GIG-BE capability. Develop initial 40 Gb connectivity among DoD testing components (GIG-BE, TSAT, Teleports) and inter-connectivity to key GIG development sites including capability to support Inter-agency end-to-end testing with DoD, Intelligence Community, Allied and Coalition activities.
- Design and test upgrade to testing suites to support 40 Gb networks
- Perform testing in support of GIG developer requirements including but not limited to:
    - IPv6 transition final testing
    - JTRS WNW end-to-end testing in support of Cluster 5 (spiral 2), AMF.
    - 40 Gbps IPv6/MPLS experimentation and testing including early HAIPE concept development
    - Support NCES spiral development
    - Continued support of end-to-end warfighter interoperability experimentation via JRAE tests in coordination with USJFCOM JBMC2 activities

  Joint C2 applications and platform testing activities such as JITC

C. Other Program Funding Summary: N/A

D. Acquisition Strategy. N/A

E. Performance Metrics:

1. User Activity and Participation. A key measurement of GIG-EF success is the amount of participation and usage of the GIG-EF in support of Joint warfighting requirements. Performance metrics in this area would include:

- Number of events, tests and experiments scheduled
- Percentage of GIG-EF time active vs. idle
- Total amount of in-kind funding from GIG developers and activities
- Aggregate funding per test

- Number of service and user participants in tests (jointness)

2. Contributions to GIG development and transition. The GIG-EF should also advance the state of the art in support of GIG implementation.
- Number of independent test reports and limited objective experiments support major GIG architectural issues (IA, IPv6/MPLS, Routing, etc.)
- Number of demonstrations in support of major GIG architectural issues (IA, IPv6, Routing, etc.)

3. Risk mitigation for the GIG.
- Demonstrations in support of GIG overall goals (ex: IPv6 by FY 2008, 10 Gb Optical HAIPE by FY 2007, etc.)
- Number of GIG E2E Systems Engineering Oversight working group requirements addressed via GIG-EF demonstration, experimentation and testing.

4. Tangible products such as frameworks and design guidance used for program assessments and reviews.

5. Specific modifications to Programs based on the frameworks and guidance that improve program compatibility and end to end performance.

6. A more collaborative environment where systems engineering organizations of individual GIG programs and the end to end systems engineering oversight organization mutually identify and solve issues related to maximizing end to end performance

Exhibit R-2, RDT&E Budget Item Justification						Date: February 2005	
Appropriation/Budget Activity RDT&E/Defense Wide BA7				R-1 Item Nomenclature: NATO Alliance Ground Surveillance (NATO AGS), PE 1001018D8Z			
Cost ($ in millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	21.475	29.689	25.474	41.268	52.593	56.496	61.588	71.887

A. Mission Description and Budget Item Justification:

(U) This project supports the U.S. share of the cost for NATO to acquire a ground surveillance capability similar to what their owned and operated Airborne Warning and Control System (AWACS) provides for air surveillance.

(U) The North Atlantic Council (NAC) validated the requirement in 1995 for a NATO-owned and operated core air-to-ground surveillance capability supplemented by interoperable national assets. Since then, the Major NATO Commanders have consistently made Alliance Ground Surveillance (AGS) their number one equipment acquisition priority.

- October 1997, NATO Conference of National Armaments Directors (CNAD) approved AGS NATO Staff Requirement (NSR)
- April 1999, NATO Washington Summit *Defense Capabilities Initiatives* (DCI) included need for a NATO-owned and operated core system for ground surveillance
- September 2001, Reinforced NAC (RNAC) re-affirmed need for a NATO-owned and operated AGS capability by 2010
- November 2002, NATO Prague Summit approved *Prague Capabilities Commitment* (PCC) that includes an airborne ground surveillance capability
- December 2003, AGS Steering Committee approved in principle the merger of NATO AGS and the Trans-Atlantic Cooperative AGS Radar (TCAR) sensor projects.
- May 2004, CNAD endorsed the Trans-Atlantic Industrial Proposed Solution consortium's selection as the program of record to enter the Design and Development Phase. The TCAR team was directed to merge with the AGS program.

(U) In May 2004, the NATO AGS Steering Committee approved an updated Master Schedule supporting a 2010 Initial Operating Capability (IOC) with Full Operational Capability (FOC) by 2013.

(U) FY 2004 Accomplishments:

Program Activities:

- Review, coordination, and staffing of Procurement Strategy for NATO AGS
- Began planning the Risk Reduction Study for the NATO AGS system
- Review, coordination, and approval of interoperability testing between NATO AGS surrogates, Joint STARS, and ASTOR systems.
- Analyses of program's radar design and integration plans for the TCAR radar
- Multinational memorandum of understanding drafted and staffed at working level
- Request for proposal drafted and staffed at working level
- Supported key International Summits and Conferences of National Armaments Directors
- Conducted follow-on feasibility analysis for trans-Atlantic development of the TCAR radar
- Attended four NATO AGS Steering Committee meetings

(U) FY 2005 Plans:

Program Activities:

- Restructure the program based on PBD 753 cuts
- Execute the initial stages of the Procurement Strategy
- Staff the Design and Development MOU
- Prepare the Design and Development contract
- Develop the SOW for the Design and Development phase
- Complete the RFP for the Design and Development phase
- Complete the Risk Reduction Study
- Secure additional funding based on establishing an executable program
- Continue interoperability efforts with the Joint STARS and ASTOR programs
- Participate in AGS Steering Committee and TCAR Executive Committee meetings

(U) FY 2006 Plans:

Program Activities:

- Execute Design and Development contract
- Participate in affordability and technical Working Groups.
- Improve and expand NATO alliance relationships relative to the industrial co-development.
- Ensure ministerial support for AGS continues
- Oversee integration testing and design work putting the TCAR radar onto the manned and unmanned platforms
- Oversee design and integration work on the ground elements of the AGS system

- Secure Congressional approval to enter into the MOU and sign Design and Development contracts

(U) FY 2007 Plans:

T&E Independent Activities:

- Provide for a professional user interface to the NATO AGS program office
- Provide radar engineers to the AGS program office
- Continue executing Design and Development Phase.
- Participate in technical and operational Working Groups.
- Improve and expand industry and professional association with NATO allies
- Address Congressional, GAO, IG Actions regarding program issues as they arise
- Ensure effective oversight of the program is provided by continuing to participate in the AGS Steering Committee

B. Program Change Summary:

	FY 2004	FY 2005	FY 2006	FY2007
Previous President's Budget	24.363	30.399	29.547	85.743
Current FY 2006 President's Budget	21.475	29.689	25.474	41.268
Total Adjustments	-2.888	-0.710	-4.073	-44.475
Congressional program reductions		-0.710		
Congressional rescissions				
Congressional increases				
Reprogrammings	-2.888		-4.073	-44.475
SBIR/STTR Transfer				
Other				

C. Other Program Funding Summary: N/A

D. Acquisition Strategy. Pending Department and Congressional approval, the U.S. will sign a Multi-national Memorandum of Understanding (MMOU) committing the government to NATO-derived shares of the Design and Development Phase in September 2005. The MMOU will support the contract and acquisition strategy now under development at the NATO AGS Support Staff in Brussels. FY 2005 funds will fund the U.S. share of a NATO AGS Risk Reduction Study.

E. Performance Metrics. NATO issues Calls for Funds generally quarterly, but often "as needed" to support its management agency decisions as they occur. Funding profile reflects anticipated US contribution that will be transferred via MIPR. The metric correlates anticipated Calls for Funds with actual MIPRs cut. Ideally, four planned calls generate four planned MIPRs. If the planned number of calls does not happen, the funding profile could be altered, and the MIPR planned workload could be altered.