Exhibit R-2, RDT&E Budget Item Justification							Date: February 2006	
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7					R-1 Item Nomenclature: Information Systems Security Program PE 0303140D8Z			
Cost ($ in millions)		FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost		11.716	12.347	14.856	13.698	13.861	13.993	14.590

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 2005 Accomplishments ($11.716 million):

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

- Continued 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.

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

- Completed the Software Assurance study and began implementation of recommendations.

- Insider Threat - CND/Information Assurance/Information Operations Attribution Capability Initiative. Leveraging work done in FY2003 and FY2004, prototyped and tested enterprise attribution and trace back tools. Demonstrated 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.

- Developed and prototyped enterprise CND, vulnerability management and situational awareness tools identified in FY2003/FY2004. Integrated output of network scanner results into Enterprise Sensor Grid (ESG) and Situational Awareness/UDOP Databases to facilitate development of ESG engineering solutions; developed initial integrated view and pilot of sensor outputs for user level control at the JTF-GNO; enhanced NSA developed prototype passive network mapping product and pilot within the JTF-GNO; developed 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; integrated/developed 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.

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

- Improved information assurance and information sharing on coalition networks through the design and development of a prototype for improving "guards" for connection between differing security domains; researched data and metadata tagging in the cross-security domain; completed the system design and implemented a prototype and software distribution portal for the client-side anonymization system.

- Identified components necessary in establishing a virtualized security data center, developed an initial "Data Center XML" (DCXML) scheme for specifying the structure of a data center configuration, and demonstrated an initial capability to automatically create a rudimentary data center for a DCXML specification.

FY 2006 Plans ($12.347 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 FY2004/05, 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: ($14.856 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.

- The DoD Software Assurance Strategy is composed of five elements: prioritization of systems, engineering-in-depth, supplier assurance, science and technology for vulnerability detection and industry outreach. The Engineering-in-depth oversight effort will allow the Defense Information Assurance Program (DIAP) to embed System Assurance Working Integrated Product Team (WIPT) within the most important acquisition programs of the Department to:

  - Assist the program manager in performing EID (review principal Systems Engineering Documents, Designs, etc.);
  - Ensure that Critical Subsystems are identified for supplier assurance and enhanced vulnerability detection;
  - Assist the program manager and Milestone Decision Authority in making risk management decisions involving Supplier threat and vulnerability mitigation.

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 2005	FY 2006	FY 2007
Previous President's Budget	10.495	12.546	12.853
Current President's Budget	11.716	12.347	14.856
Total Adjustments	1.221	-.199	2.003
Congressional program reductions			
Congressional rescissions, Inflation adjustments	-.279	-.199	2.003
Congressional increases			
SBIR/STTR Transfer			
Reprogrammings	1.500		

Change Summary Explanation:
FY 2005: Reprogramming from NSA 1.500 million; SBIR -.237 million; STTR -.028; Atomic Energy -.008 million; WHS reduction -.006 million.
FY 2006: FFRDC -.020 million; Economic Assumptions -.054 million; Rescission -.125 million.
FY 2007: Non-Pay Purchase Inflation .203 million; Software Assurance 1.800 million.

C. **Other Program Funding Summary**:

								Total
	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Cost
O&M, DW (PE0303140D8Z)	20.681	19.512	16.200	16.097	17.977	17.931	16.935	142.078

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.