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.