Exhibit R-2, RDT&E Budget Item Justification							Date: February 2007	
Appropriation/Budget Activity RDT&E Defense-Wide, BA 7				R-1 Item Nomenclature: Information Systems Security Program PE 0303140D8Z				
Cost ($ in millions)	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Total PE Cost	12.048	17.654	13.256	13.491	13.708	14.205	14.426	14.649

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 2006 Accomplishments ($12.048 million):

- Completed development of Enterprise Mission Assurance Support System (eMASS) (v1.0) into a deployed enterprise certification and accreditation management tool and provided as piloted IA Core Enterprise Service. Completed initial development and deployment of a complimentary IA Knowledge Service providing the technical underpinnings of the DoD Information Assurance Security Controls required to support the DoD Certification and Accreditation Process

- Continue refinement of IA architecture, policy and IA capabilities necessary to support and "end-to-end" IA capability for the Global Information Grid (GIG) – including enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Released version 1.1 of the IA Component of the GIG Architecture. Provided IA system engineering support to the Global Information Grid System Engineering effort.

- Leveraging work done in FY2005/06, continued experimentation, technology demonstration, prototype and test of attribution, anomaly detection, trace-back, CND response action tools, with emphasis on DoD enterprise level application. Continued to pilot specific operational capability to identify and characterize intruder behavior in DoD networks.

- Initiated planning and CONOP development to integrate TRICKLER, a passive monitoring tool, on the NIPRNet and SIPRNet to increase situational awareness of vulnerable, misconfigured, and unauthorized systems on the network. Initiated a pilot with the Army to develop and refine the CONOPS and Tactics, Techniques and Procedures through lessons learned by deploying TRICKLER at the installation level.

- Continued the evaluation, selected research, and focused piloting/investigation of various emerging IA capabilities (e.g., cross-domain, vulnerability management, situational awareness technologies, tools and techniques) to improve the IA and CND posture of the Department of Defense and support net-centric development. Began pilot to examine integration of DISA Field Security Operations Security Readiness Review and the Counterintelligence Field Activity (CIFA) Defensive Counterintelligence Assessment (DCA to evaluate the feasibility of conducting SRR blue-team technical assistance visits with the Insider Threat focused DCA identification & evaluation process This integrated review will leverage complementing SRR and DCCA capabilities to provide a more streamlined and comprehensive evaluation of information security practices

- CND Architecture: developed DOD Architectural Framework artifacts for the Computer Network Defense Referenced Architecture that provided input and guidelines to the GIG IA and NETOPS Architectures. These views also provide a baseline for Component CND Architects to integrate and implement an architecture that will provide a cohesive enterprise architecture maximizing the capabilities of the DOD enterprise-wide CND solutions and facilitate Joint Forces Command's CONOPS development. This included: AV - 2 (Integrated Dictionary), OV-5 (Operational Activity Model), OV-7 (Logical Data Model) (SV1 -System Interface Descriptions (for ESSG procured tools).

- Expanded the work on the CND Architecture Logical Data Model to initiate data strategy efforts under a CND Community of Interest (COI). Through this effort the CND Community has started to develop logical data models to include entity definitions, use cases, and relationship diagrams as well as beginning to define a CND ontology to enable improved net-centric information sharing within the CND community.

- Studied and developed a proof of concept to manage, track, and trace CND requirements using standard architectural tools (e.g., DOORS software suite) from a top-down and bottom-up point of view point. This concept allows the

CND community to easily trace and align requirements between the architecture and the immediate requirements in the field as well as supports the DOD JCIDS and NCIDS processes. This effort supports the architecture development specifically for the AV-1, SV-3, SV-5, OV6A, TV-1, TV-2

- Developed Software Assurance (SwA) processes and procedures for implementing the DoD SwA Strategy, including prioritization, engineering-in-depth, supplier assurance, and application of intelligence and security capabilities to counteract and risk manage supply chain threat to the acquisition of critical systems.

- Began pilot of capabilities of web logging and data analysis tool(s) in a coalition sharing environment to collect and aggregate raw log data from any connected data source, analyze that data in real time, set alerts to warn of suspicious/anomalous behavior and store data for on-demand retrieval. Includes assessing ability of commercial tools for (a) real time and historical trend analysis, (b) capability to identify and isolate risks, (c) capability to aggregate high volume data, (d) capability for rapid search and analysis for compliance and threat mitigation, and (e) automating log data archival and providing secure data retention.

.

- Continued development of the DoD IA Portal, including ability to support a variety of enterprise level IA tools, including IA knowledge Service, secure configuration compliance verification and remediation.

FY 2007 Plans: ($17.654 million)

- $2.900 million Congressional Add, Code Assessment & Metholology Project (CAMP) - Reprogramming to NSA.

- 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. Examine technical approaches to improving data at rest protection and addressing data aggregation issues.

- Continue experimentation, technology demonstration, prototype and test evolving CND/situational awareness, vulnerability management, attribution, anomaly detection, trace back and response tools.. Pilot the CNDSP Measure of Effectiveness Program through evaluation of five Components and their CNDSP and upon validation transition the

program to the DOD Blue/Red Teams.

- CND Architecture: Expand the System View (SV-1, SV4) to include emerging CND tools and capabilities (e.g. Host Based Security Suite, TRICKLER, Insider Threat tools): expand the Architecture Views to include the [SV10C (Systems Event-Trace), the SV-3 (Systems-Systems Matrix, the OV -6C (Operational Event-Trace), TV-1, TV-2 (Technical Standards Profile and Forecast)

- Conduct a DoD CND COI Pilot to demonstrate net-centric data sharing in a Service Oriented Enterprise Architecture. The pilot will include DISA, NSA, Army, and AF participation evaluating net-centric sharing and correlation of sensor data (limited platforms in 07), vulnerability data, asset data, patch management data, and incident data. Incorporate the TRICKLER data strategy to integrate TRICKLER into the CND User Defined Operational Picture in order to have real-time situational awareness through visual tools to defend DoD networks.

- Begin implementation of the DoD Software Assurance Strategy by piloting key aspects of the Engineering Support Program to manage software assurance risk, e.g., develop the ability to identify critical subsystems for supplier assurance, determine the key elements of engineering-in-depth. The 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 embed a System Assurance Working Integrated Product Team (WIPT) within the most important acquisition programs of the Department to (1) assist the program manager in performing EID (review principal systems engineering documents, designs, etc.); (2) ensure that critical subsystems are identified for supplier assurance and enhanced vulnerability detection; and (3) assist the program manager and Milestone Decision Authority in making risk management decisions involving supplier threat and vulnerability mitigation.

FY 2008 Plans: ($13.256 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.

- Further develop and refine engineering-in-depth and vulnerability detection to support the DoD Software Assurance Strategy.

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

FY 2009 Plans: ($13.491 million)

- 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.

- Further develop and refine engineering-in-depth and vulnerability detection to support the DoD Software Assurance Strategy.

- 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 2006	FY 2007	FY 2008	FY 2009
Previous POM/BES	12.347	14.856	13.256	13.491
Current Presidents Budget	12.048	17.654	13.256	13.491
Total Adjustments	-.299	2.798		
Congressional program reductions				
Congressional rescissions, Inflation adjustments	-.299	-.102		
Congressional increases		2.900		
SBIR/STTR Transfer				
Reprogrammings				

Change Summary Explanation:
FY 2006: SBIR -.267 million, STTR -.032 million.
FY 2007: Congressional Add 2.900 million, FFRDC -.035 million, Economic Assumptions -.067 million.
FY 2008: No change.
FY 2009: No change.

C. **Other Program Funding Summary**:

	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY2013	Total Cost
O&M, DW (PE0303140D8Z)	18.529	15.696	16.690	18.025	18.133	17.208	17.526	17.841	139.648

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.