Exhibit R-2, RDT&E Budget Item Justification						Date: February 2008	
Appropriation/Budget Activity RDT&E, Dw BA 07			R-1 Item Nomenclature: Information Systems Security Program, 0303140D8Z				
Cost ($ in millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Total PE Cost	18.204	15.524	13.459	13.579	14.066	14.287	14.508
Information Systems Security Program, P140	18.204	15.524	13.459	13.579	14.066	14.287	14.508

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 2007 Accomplishments: ($18.204 million)

- $2.900 million Congressional Add, Code Assessment & Methodology Project (CAMP) - Reprogramming to NSA.
- Converted eMASS into a Core Enterprise Service information assurance management tool.
- Continued 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. Examined technical approaches to improving data at rest protection and addressing data aggregation issues.

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2008
Appropriation/Budget Activity RDT&E, Dw BA 07	R-1 Item Nomenclature: Information Systems Security Program, 0303140D8Z

- Continued experimentation, technology demonstration, prototype and test evolving CND/situational awareness, vulnerability management, attribution, anomaly detection, trace back and response tools. Piloted 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: Expanded 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)

- Conducted a DoD CND COI Pilot to demonstrate net-centric data sharing in a Service Oriented Enterprise Architecture. The pilot included 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. Incorporated 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.

- Began 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.

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2008
Appropriation/Budget Activity RDT&E, Dw BA 07	R-1 Item Nomenclature: Information Systems Security Program, 0303140D8Z

FY 2008 Plans: ($15.524 million)

- $2.400 million Congressional Add for Security for Critical Communications Networks (SCCN). This program entails the systematic network embedding of hardware monitoring units optimized for security activities and partnering with the existing network components to achieve "built-in" network security for DoD applications.

- 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: ($13.459 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.

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2008
Appropriation/Budget Activity RDT&E, Dw BA 07	R-1 Item Nomenclature: Information Systems Security Program, 0303140D8Z

B. Program Change Summary:

	FY 2007	FY 2008	FY 2009
Previous President's Budget	17.654	13.256	13.491
Current Budget Estimates Submission	18.204	15.524	13.459
Total Adjustments	0.550	2.268	-0.032
Congressional decreases	0	-0.132	0
Congressional increases	0	2.400	0
Reprogrammings	0	0	0
SIBR/STTR Transfer	0	0	0
Other	0.550	0	-0.032

Change Summary Explanation: N/A

FY 2007: Rounding adjustments at the Department level .550 million.
FY 2008: Congressional Add $2.400 million, FFRDC -$0.036 million, Contractor Efficiencies -$0.025 million, Economic Assumptions $-0.071 million.
FY 2009: Program adjustments of -$0.032 million.

C. Other Program Funding Summary: N/A

	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	To Complete	Total Cost
O&M, DW (PE0303140D8Z)	17.718	16.356	17.851	18.133	17.208	17.526	17.841	Continuing	122.633

D. Acquisition Strategy: N/A

Exhibit R-2, RDT&E Budget Item Justification	Date: February 2008
Appropriation/Budget Activity RDT&E, Dw BA 07	R-1 Item Nomenclature: Information Systems Security Program, 0303140D8Z

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.