

Exhibit R-2, RDT&E Budget Item Justification				Date: May 2009
Appropriation/Budget Activity RDT&E DW/BA # 7			R-1 Item Nomenclature: Information Systems Security Program/0303140D8Z	
Cost (\$ in millions)	FY 2008	FY 2009	FY 2010	
Total PE Cost	15.125	13.386	13.477	
<p><b>A. Mission Description and Budget Item Justification:</b>                      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.</p> <p>FY 2008 Accomplishments: (\$15.125 million)</p> <ul style="list-style-type: none"> <li>• \$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.</li> <li>• Converted eMASS into a Core Enterprise Service information assurance management tool.</li> <li>• 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.</li> <li>• Developed and implemented; a demonstration of standards-based binary vulnerability detection Guidebook for Systems Engineering for Systems Assurance; a strategic approach to prioritize Systems and Networks for enhanced SCRM; a baseline of practices and procedures for Supply Chain Risk Management (SCRM) across the lifecycle and the DoD SCRM; and an approach for identifying gaps.</li> </ul>				

UNCLASSIFIED

- Developed a strategic plan; for performing monitoring and oversight; and metrics for identifying and prioritizing provisions of national security agreements for monitoring and oversight; for standardizing nomenclature for describing incremental risk within CFIUS transactions.
- Developed and refined engineering-in-depth and vulnerability detection to support the DoD Software Assurance Strategy.
- Developed the Consolidated Exercise Metrics Assessment Tool (CEMAT), a test and evaluation “data collector in a box” capability; DISA/JITC successfully piloted the alpha version for proof of concept during BULWARK DEFENDER 08
- Upgraded the Security Assessment Simulation Toolkit (SAST) to a beta version; used by the USMC as their traffic simulation tool for the range portion of BULWARK DEFENDER 08, and used by DISA as an integral component of their RaDX training capability. As a result, the US Navy is planning to adopt SAST for BULWARK DEFENDER 09, and AFCA is incorporating portions into their SIMTEX/JCOR capability.
- Developed an assessment methodology for CND Service Provider’s (CND/SP) for five DoD components to measure the current state of CND/SP effectiveness in identifying and understanding which malicious activities are being correctly identified and which are not, which will also feed into sensor placement needs and CNDSP analyst training needs.
- Developed CND data-standards and web-services to support the re-engineering of JTF-GNO’s IAVM processes, which are being used as the baseline for NETOP data-standards, and GIG Enterprise asset reporting initiatives which are directed by the CDR of DISA JTF-GNO.
- Developed a pilot plan to implement Interrogator sensors and analyst support at key points across the network that will validate the Interrogator capability in different instantiations that range from large network connection points, key low bandwidth tactical sites to web portals to strategic command sites.

FY 2009 Plans: (\$13.386 million)

- Continue refinement of IA architecture, policy and IA capabilities necessary to support “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.

UNCLASSIFIED

R-1 Line No. 193

Page 2 of 4

UNCLASSIFIED

- Continue refinement of SAST to provide more robust and realistic T&E, training and exercise environment. Improvements include creation of a virtual or “fake” internet, instrumentation to support CEMAT collection capabilities, DoD CAC Engine and new traffic protocols in support of IA joint exercises and the Department’s international exercise program.
- Continue refinement of CEMAT for automated test/exercise data collection, reduction and analysis
- Pilot an IA/CND exercise and training workshop among multiple nations, of various technical skill and capability levels and perform a technology demonstration of SAST and proof-of-concept of distributed CND exercise and training focusing on “train-as-you-fight” techniques and advance partner nation collaboration.
- Develop national supply chain risk management plan to mitigate threats to software/hardware to USG information communications and technology infrastructure.
- Develop a pilot plan for authority based access control (ABAC).
- Finalize NATO and European agreements to expand bilateral sharing agreements fro incident and threat information sharing.
- Continue CND improvements for the Integration and Certification of CND Pilot to support interoperability and operational initiatives including additional data feeds, small agency asset SCAP data collection, authentication and authorization, SCAP remediation standards and continued development/validation of CND data-standards.

FY 2010 Plans: (\$13.477 million)

- Continue refinement of IA architecture, policy and IA capabilities necessary to support “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 refinement of SAST to provide more robust and realistic T&E, training and exercise environment. Improvements include creation of a virtual or “fake” internet, instrumentation to support CEMAT collection capabilities, DoD CAC Engine and new traffic protocols in support of IA joint exercises and the Department’s international exercise program.

UNCLASSIFIED

R-1 Line No. 193

Page 3 of 4

- Continue refinement of CND improvements for integration and certification to support interoperability and operational initiatives including additional data feeds, small agency SCAP data collections, authentication and authorization, SCAP remediation standards and continued development/validation of CND data-standards.

**B. Program Change Summary:**

	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>
Previous Presidents Budget	15.524	13.459	13.579
Current Presidents Budget	15.125	13.386	13.477
Total Adjustments	-0.399	-0.073	-0.102
Congressional program reductions			
Congressional rescissions			
Congressional increases			
Reprogrammings			
SIBR/STTR Transfer			
Program Adjustments	-0.399	-0.073	-0.102
PBD Adjustments			

Program Change Explanation:

FY 2008: Program adjustment.

FY 2009: Program adjustment.

FY 2010: Program adjustment.

**C. Other Program Funding Summary:**

	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>
O&M, DW (PE0303140D8Z)	16.527	17.443	16.520

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

**E. Performance Metrics:**

- SAST supports CEMAT capability
- SAST available as a core enterprise IA/CND simulation tool
- CEMAT effectively supports T&E community data collection, reduction, analysis and reporting