

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY			R-1 ITEM NOMENCLATURE								
0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>			PE 0303140D8Z: <i>Information Systems Security Program</i>								
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
Total Program Element	13.658	11.352	11.780	-	11.780	12.163	12.433	12.514	12.741	Continuing	Continuing
140: <i>Information Systems Security Program</i>	13.658	11.352	11.780	-	11.780	12.163	12.433	12.514	12.741	Continuing	Continuing
Quantity of RDT&E Articles											

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.

B. Program Change Summary (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Previous President's Budget	14.077	11.753	11.703	-	11.703
Current President's Budget	13.658	11.352	11.780	-	11.780
Total Adjustments	-0.419	-0.401	0.077	-	0.077
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program Adjustment	-0.419	-	0.077	-	0.077
• FFRDC Reduction	-	-0.078	-	-	-
• SBIR Reduction	-	-0.285	-	-	-
• STTR Reduction	-	-0.038	-	-	-

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

Change Summary Explanation

FY 2011: Includes Studies Contractor Efficiency -1.169 million, Service Support Contract Efficiency -0.357 million, Program adjustment -0.419 million.
 FY 2012: FFRDC reduction -0.078 million, SBIR reduction -0.258 million, STTR reduction -0.038 million.
 FY 2013: Program Adjustment 0.077 million.

Studies contract Efficiencies will be realized by reducing the number of studies that we participate in while still supporting enterprise-wide information technology goals critical to DoD Mission.
 Service Support Contract efficiencies will be realized by reducing the reliance on DoD Service Support Contractors by utilizing in-house government support in a constrained personnel and resource environment.

C. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012	FY 2013
<p>Title: Information Systems Security Program Plans and Accomplishments</p> <p>FY 2011 Accomplishments:</p> <ul style="list-style-type: none"> • Continued 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 to long term increment of the IA Component of the GIG Architecture. • Developed central engineering in-depth concept of criticality analysis, and Concept of Operations for leveraging criticality analysis to guide use of intelligence resources to support the DoD trusted defense system strategy (including Software and Hardware Assurance). Applied criticality analysis within USD(AT&L) program protection planning engagements • Continued refinement of SAST (now called Zanthemon Inductive User Interface) 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. • Completed Phase I of Cyber Challenge, the Department’s FY13 annual awareness training product. • Continued 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. • Provided essential support to DoD Information Assurance (IA) Risk Management (RM) Transformation that included migrating the Defense IA RM process to comply with the mandated Federal (NIST) community RM standards, performing the functions 	13.658	11.352	11.780

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013
<p>of the DIACAP TAG Secretariat IAW DoD 8510.01, supporting enterprise-wide IA RM automation (eMASS) requirements identification and implementation, and managing DoD's single, virtual, authoritative community of interest for DoD IA RM policies, activities, and initiatives known as the DIACAP Knowledge Service.</p> <ul style="list-style-type: none"> • Developed the DoD Mobile Device Strategy and Roadmap, to include policy and IA capabilities necessary to support "end-to-end" IA capability for the GIG-including mobile enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Support mobile technology demonstrations, development and pilots focused on functions required in mid to long term increment of the IA Component of the GIG Architecture. • Developed and refined the DoD policy for Digital Persona Protection to include the construction of an implementation plan based on the final policy to support workforce protection awareness, education and training throughout the department. • Researched and developed DoD policies related to wireless, emerging technologies and mobile computing while to ensure the security standards and policies are implemented with legacy and cutting edge technologies in mind throughout their entire life-cycle. • Provided IA Mobile Enterprise Services support in the development of DoD-enterprise cloud computing adoption strategy as the DoD Mobile Device Strategy and Roadmap will work in lockstep with the cloud computing strategy. • Delivered two DoD level signed policies: DoD Instruction 8520.02 "PKI and PK-Enabling" and a new DoD Instruction 8520.03-"Identity Authentication." The new policies commit the Department to adopt the use of PKI-based capabilities internally in business processes and externally with DoD commercial partners and require DoD systems to use stronger authentication solutions, reducing anonymity on DoD networks. • Lead the DoD SHA-256 Migration Coordination Cell. Support development and implementation of the SHA-256 Cryptographic migration plan. The migration plan directs transitioning the DoD IT infrastructure to support the use of the SHA-256 hash algorithm. • Developed processes to quickly identify the alignment of DoD Components networks and information systems to a certified and accredited CNDSP in accordance with the Department of Defense Directive (DoDD) 8530.1. • Evolved and document the assessment methodology for conducting Measures of Effectiveness (MOE) of CNDSPs and apply across the DoD to assess the quality and effectiveness of CND services coverage over specific DoD component networks and information systems. 			

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013
---	----------------	----------------	----------------

- Expanded the International Cyber Defense Workshop bi-annual events to cover two time zone and more nations; operationalized IA/CND relationships with France, Sweden and Poland.
 - Developed and circulated of Cloud Security Architecture to compliment the Defense Cloud Strategy
 - Continued to assess and design solutions to enhance the resiliency of the GIG, including the analysis of communications paths, and the design of robust DoD systems to withstand sophisticated cyber attacks and cyber outages.
 - Continued to develop capabilities to enhance cyber awareness throughout the GIG, including the delivery of enterprise network mapping and leak detection system (ENMLDS) capabilities.
 - Lead in the augmentation of the C&A process to leverage the NIST 800-53 security controls, and collaborate with members of the Intelligence Community in the development of cross-community security profiles to aid in the accreditation of systems across the DoD and IC.
- FY 2012 Plans:**
- 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 to long term increment of the IA Component of the GIG Architecture.
 - Continue to provide essential support to DoD Information Assurance (IA) Risk Management (RM) Transformation that includes migrating the Defense IA RM process to comply with the mandated Federal (NIST) community RM standards, performing the functions of the DIACAP TAG Secretariat IAW DoD 8510.01, supporting enterprise-wide IA RM automation (eMASS) requirements identification and implementation, and managing DoD's single, virtual, authoritative Community of Interest (known as the DIACAP Knowledge Service) for DoD IA RM policies, activities, and initiatives.
 - Further develop, refine and deploy criticality analysis in support the DoD trusted defense system strategy (including Software and Hardware Assurance).
 - Complete Phases 3 & 4 of the Zanthenon Inductive User Interface (formerly known as SAST) GUI to enhance ease of use and permit independent development, testing and maintenance of T&E, training and exercise scenarios. Improvements will support joint exercises, the Department's international exercise program, and capstone events at Service schools.

FY 2011	FY 2012	FY 2013

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013
<ul style="list-style-type: none"> • Pilot ICDW-like training exercise for DoD agencies. • Complete Phase II of Cyber Challenge, the Department’s FY 2013 annual awareness training product. • Automate CEMAT capabilities in the IA Range. • Develop 508 solution for VTE content. • Continue refinement of the DoD Mobile Device Strategy and Roadmap, to include policy and IA capabilities necessary to support "end-to-end" IA capability for the GIG-including mobile enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Support mobile technology demonstrations, development and pilots focusing functions required in mid to long term increment of the IA Component of the GIG Architecture. • Further develop and refine the DoD policy for Digital Persona Protection to include the construction of an implementation plan based on the final policy to support workforce protection awareness, education and training throughout the department. • Continue to refine and update DoD policies related to wireless, emerging technologies and mobile computing while to ensure the security standards and policies are implemented with legacy and cutting edge technologies in mind throughout their entire life-cycle. • Continue to provide IA Mobile Enterprise Services support to further develop and refine the DoD-enterprise cloud computing adoption strategy as the DoD Mobile Device Strategy and Roadmap will work in lockstep with the cloud computing strategy. • Support and monitor implementation of the SHA-256 Cryptographic migration. • Provide policy and guidance for the use of Federal PIV and non-Federal PIV-I credentials within the DoD for mission applications and business functions. • Respond to inquiries from DoD Customers and Information system owners regarding DoD PKI and Identity Management policy and guidance. • Collaborate with CYBERCOM to develop implementation guidance for DoD PKI and Identity Management policy. 			

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013
<ul style="list-style-type: none"> • Improve the International Cyber Defense Workshop virtual environment by moving the portals and SAST to the .mil domain; conclude information sharing agreement with Finland and provide more IA/CND information in releasable form to all formal international partners (NATO, FVEY, Japan, ROK, Singapore, France, Germany, Poland, Sweden). <p><i>FY 2013 Plans:</i></p> <ul style="list-style-type: none"> • Develop products and test tools for a comprehensive cybersecurity awareness program. • Extend ICDW-like training exercises to all DoD agencies. • Continue Zanthenon GOTS API/SDK enhancements. • Continue to provide essential support to DoD Information Assurance (IA) Risk Management (RM) Transformation that includes migrating the Defense IA RM process to comply with the mandated Federal (NIST) community RM standards, performing the functions of the DIACAP TAG Secretariat IAW DoD 8510.01, supporting enterprise-wide IA RM automation (eMASS) requirements identification and implementation, and managing DoD's single, virtual, authoritative Community of Interest (known as the DIACAP Knowledge Service) for DoD IA RM policies, activities, and initiatives. • Continue refinement of the DoD Mobile Device Strategy and Roadmap, to include policy and IA capabilities necessary to support "end-to-end" IA capability for the GIG-including mobile enterprise services such as discovery, collaboration, messaging, mediation, data tagging, etc. Support mobile technology demonstrations, development and pilots focusing functions required in mid to long term increment of the IA Component of the GIG Architecture. • Further develop and refine the DoD policy for Digital Persona Protection to include the construction of an implementation plan based on the final policy to support workforce protection awareness, education and training throughout the department. • Continue to refine and update DoD policies related to wireless, emerging technologies and mobile computing while to ensure the security standards and policies are implemented with legacy and cutting edge technologies in mind throughout their entire life-cycle. • Continue to provide IA Mobile Enterprise Services support to further develop and refine the DoD-enterprise cloud computing adoption strategy as the DoD Mobile Device Strategy and Roadmap will work in lockstep with the cloud computing strategy. • Develop Advanced Persistent Threat (APT) data standards and data collection capabilities 			

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Office of Secretary Of Defense **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 0400: <i>Research, Development, Test & Evaluation, Defense-Wide</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140D8Z: <i>Information Systems Security Program</i>
---	--

C. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013
<ul style="list-style-type: none"> • Pilot NIPRNet – Internet isolation capabilities. • Expand scope of International Cyber Defense Workshop to include more training modules and expanded IA range capabilities in SAST model; develop web portals for classified FVEY information sharing and methodologies for releasing IA/CND information to formal partners in near real time. 			
Accomplishments/Planned Programs Subtotals	13.658	11.352	11.780

D. Other Program Funding Summary (\$ in Millions)

Line Item	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
• 0303140D8Z: <i>Information System Security Program</i>	26.043	13.772	13.021		13.021	12.947	13.195	13.673	106.576	Continuing	Continuing

E. Acquisition Strategy
N/A

F. Performance Metrics

- Zanethenon improvements available as a core enterprise IA/CND simulation tool
- CEMAT effectively supports T&E community data collection, reduction analysis and reporting.
- 508 solution available for VTE content.
- Cyber Challenge used DoD-wide.
- DoD agency CIOs report ICDW-like training exercises are valuable tool to enhance cybersecurity skills of personnel.