Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
Total Program Element	11.348	10.496	10.638	11.304	-	11.304	10.127	9.896	10.683	11.387	Continuing	Continuing
140: *Information Systems Security Program*	11.348	10.496	10.638	11.304	-	11.304	10.127	9.896	10.683	11.387	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The The DoD CIO 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.DoD CIO 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

B. Program Change Summary ($ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	11.780	10.673	12.867	-	12.867
Current President's Budget	10.496	10.638	11.304	-	11.304
Total Adjustments	-1.284	-0.035	-1.563	-	-1.563
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Sequestration Reduction	-0.969	-	-	-	-
• Efficiencies Reduction	-	-	-1.563	-	-1.563
• SBIR/STTR Reduction	-0.310	-	-	-	-
• Program Reduction	-0.005	-	-	-	-
• FFRDC Reduction	-	-0.035	-	-	-

Change Summary Explanation

Program Change Explanation:
FY 2013: Sequestration Reduction -0.969 million, SBIR/STTR reduction -0.310 million, Program adjustment-0.005 million.
FY 2014: FFRDC Reduction -0.035 million.
FY 2015: Efficiency reduction -1.563 million.

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Information Systems Security Program Plans and Accomplishments	10.496	10.638	11.304
FY 2013 Accomplishments: Developed products and test tools for a comprehensive cybersecurity awareness program, and extended cyber defense training exercises to all DoD agencies. • Continued CND Architecture and Capability development. • Provided 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			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
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. • Refined 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. • Developed DoD policy for Digital 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. • Refined and updated 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 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. • Developed Advanced Persistent Threat (APT) data standards and data collection capabilities • Piloted NIPRNet – INTERNET isolation capabilities. • Expanded the scope of the International Cyber Defense Workshop to include more training modules and expanded IA range capabilities in SAST model; developed web portals for classified five-eyes (FVEY) information sharing and methodologies for releasing IA/CND information to formal partners in near real time. • Performed Continuous Monitoring and Risk Scoring (CM/RS); developed the strategy and objectives for institutionalizing continuous monitoring across DoD; coordinated CM/RS capabilities; and prepared applicable CM/RS issuances. • Provided strategic management and oversight of the Computer Network Defense Service Provider (CNDSP) Program; and conducted trend analysis to identify systemic trends and associated gaps to the CNDSP program. • Researched PKI interoperability policy, governance, and interoperability implementation recommendations to incorporate PKI and strong identity technologies in cyber environments to support DoD and Warfighter operations.			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
• Developed Cross Domain (CD) technical & acquisition expertise (e.g., CD investment strategy, and CD enterprise capability). • Developed, coordinated and supported a series of Cyber initiatives and associated issue papers for the POM-15 Resource Management Decision (RMD) process that will provide resources to DISA, NSA, DOD-CIO, and the Services. • Conducted a series of Cyber and Information Assurance program reviews with the Services, DISA, and NSA to address program implementation and resourcing status. • In support of the DOD CNDSP Program, conducted a series of technical & operational Measures of Effectiveness (MOE) Evaluations to address effectiveness of the CNDSPs implementation of DODD/I-8530.1/.2. Results of the MOE also facilitated the success of Component Command Cyber Readiness Inspections (CCRIs) as directed to be accomplished by USCYBERCOM. • Developed, coordinated, and maintained Cyber metrics for reporting to DOD-CIO, DCMO and other organizations as necessary.			
FY 2014 Plans: Continue development of capabilities (products and test tools, etc.,) for a comprehensive cybersecurity awareness program. • Continue cyber-defense training exercises for all DoD agencies. • Continue research, analyses, and development of education, training, and awareness concepts and course-contents related to SCRM, HwA, SwA, and Assured Services (and associated SCRM Standards with respect to people-process-technology-metrics) • Research, analyses, and development of concepts for consistent protection from supply chain exploitation and attack within/by individual acquisitions and procurements of DoD materiel and services on which DoD systems, networks, and missions depend. • Monitor the on-going implementation of SCRM key practices and test and evaluation processes across DoD. • Continue to provide essential support to DoD Information Assurance (IA) Risk Management (RM) Transformation: 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; support for the enterprise-wide IA RM automation (eMASS) requirements identification and implementation; and management of the DoD single, virtual, and authoritative Community of Interest (known as the DIACAP Knowledge Service) for DoD IA RM policies, activities, and initiatives.			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
• Continue the 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. • Continue the refinement of the DoD policy for Digital Protection, to include research and development of an implementation plan IAW the final policy on workforce protection awareness, education, and training. • Continue to research and refine DoD policies on wireless, emerging technologies and mobile computing while ensuring security standards and policies are implemented with both legacy and emerging technologies in mind throughout their entire life-cycle. • Research and refine Advanced Persistent Threat (APT) data standards and data collection capabilities • Provide strategic management and oversight of the CNDSP Program; and conduct trend analysis to identify systemic trends and associated gaps in the CNDSP program. • Support DODD/I-8530 .1/.2 with CNDSP evaluations and Conduct Measures of Effectiveness (MOE) Evaluations to address effectiveness of the CNDSPs implementation of DODD/I-8530.1/.2, and to address cyber security issues identified by USCYBERCOM. • Conduct Cyber Security program reviews with the Services, DISA, & NSA to address program implementation and resourcing issues and requirements. • Conduct Portfolio Reviews of Cybersecurity initiatives addressing Component cost, schedule, and performance of ISSP funded initiatives. • Develop, coordinate, and support Cyber initiatives and associated issue papers for the POM-16 Resource Management Decision (RMD) process that will provide resources to DISA, NSA, DOD-CIO, and the Services. • Develop, coordinate, and maintain Cyber metrics for reporting to DOD-CIO, DCMO and other organizations as necessary. • Continue research and refinement of IPv6 compatibility across NIPRNet; and ensuing implementation guidance. • Continue participation in the research, development, and implementation of DoD DMZ Increment engineering plans, to include monitoring the on-going implementation of NIPRNet DMZs and migration of outward facing applications.			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
• Continue implementation and refinement of NIPRNet and SIPRNet Mapping and Leak Detection Solution to identify vulnerabilities and develop risk mitigation strategy. • Monitor the software engineering and implementation of the advanced Whitelisting database capability to reduce NIPRNet exposure to the Internet. • Expand the scope of the International Cyber Defense Workshop to include more training modules and develop new IA range capabilities for the virtual workshop; develop methodologies for releasing IA/CND information to formal partners in near real time. • Continue collaboration with Combatant Commands (COCOMs) to support the identification and prioritization of cleared companies providing operational support and thereby assist and promote their full participation when the DIB CS/IA voluntary program opens to all cleared defense contractors. • Monitor the DIB CS/IA program expansion under FVEY CND MOU and any International amendments to the Framework Agreement. ***FY 2015 Plans:*** Continue development of capabilities (products and test tools, etc.,) for a comprehensive cybersecurity awareness program. • Continue cyber-defense training exercises for all DoD agencies. • Continue research, analyses, and development of education, training, and awareness concepts and course-contents related to SCRM, HwA, SwA, and Assured Services (and associated SCRM Standards with respect to people-process-technology-metrics) • Research, analyses, and development of concepts for consistent protection from supply chain exploitation & attack within/by individual acquisitions and procurements of DoD materiel and services on which DoD systems, networks, and missions depend. • Monitor the on-going implementation of SCRM key practices and test and evaluation processes across DoD. • Continue to provide essential support to DoD Information Assurance (IA) Risk Management (RM) Transformation: 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; support for the enterprise-wide IA RM automation (eMASS) requirements			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
identification and implementation; and management of the DoD single, virtual, and authoritative Community of Interest (known as the DIACAP Knowledge Service) for DoD IA RM policies, activities, and initiatives. • Continue the 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. • Continue the refinement of the DoD policy for Digital Protection, to include research and development of an implementation plan IAW the final policy on workforce protection awareness, education, and training. • Continue to research and refine DoD policies on wireless, emerging technologies and mobile computing while ensuring security standards and policies are implemented with both legacy and emerging technologies in mind throughout their entire life-cycle. • Research and refine Advanced Persistent Threat (APT) data standards and data collection capabilities • Provide strategic management and oversight of the CNDSP Program; and conduct trend analysis to identify systemic trends and associated gaps to the CNDSP program. • Continue research and refinement of IPv6 compatibility across NIPRNet; and ensuing implementation guidance. • Continue participation in the research, development, and implementation of DoD DMZ Increment engineering plans, to include monitoring the on-going implementation of NIPRNet DMZs and migration of outward facing applications. • Continue implementation and refinement of NIPRNet and SIPRNet Mapping and Leak Detection Solution to identify vulnerabilities and develop risk mitigation strategy. • Monitor the software engineering and implementation of the advanced Whitelisting database capability to reduce NIPRNet exposure to the Internet. • Continue collaboration with Combatant Commands (COCOMs) to support the identification and prioritization of cleared companies providing operational support and thereby assist and promote their full participation when the DIB CS/IA voluntary program opens to all cleared defense contractors.			

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*

C. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
• Monitor the DIB CS/IA program expansion under FVEY CND MOU and any International amendments to the Framework Agreement. • Expand the scope of the International Cyber Defense Workshop to include more training modules and continue to develop new IA range capabilities for the virtual workshop; develop methodologies for releasing IA/CND information to formal partners in near real time. • Support DODD/I-8530.1/.2 for CNDSP evaluations and Conduct Measures of Effectiveness (MOE) Evaluations to address effectiveness of the CNDSPs implementation of DODD/I-8530.1/.2. and cyber security issues identified by USCYBERCOM. • Conduct Cyber Security program reviews with the Services, DISA, and NSA to address program implementation and resourcing issues and requirements. • Conduct Portfolio Reviews of Cyber security initiatives addressing Component cost, schedule, and performance of ISSP funded initiatives. • Develop, coordinate, and support Cyber initiatives and associated issue papers for the POM-16 Resource Management Decision (RMD) process that will provide resources to DISA, NSA, DOD-CIO, and the Services. • Develop, coordinate, and maintain Cyber metrics for reporting to DOD-CIO, DCMO and other organizations as necessary.			
Accomplishments/Planned Programs Subtotals	10.496	10.638	11.304

D. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• 0303140D8Z O&M DW: *Information System Security Program*	13.253	13.178	11.509	-	11.509	12.255	12.485	12.159	11.805	Continuing	Continuing

Remarks

E. Acquisition Strategy

N/A

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Office of Secretary Of Defense	Date: March 2014
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140D8Z *I Information Systems Security Program*

F. Performance Metrics

Zanethenon improvements available as a core enterprise IA/CND simulation tools.

- CEMAT effectiveness in supporting the T&E community for data collection, reduction analysis, and reporting.
- 508 solution available for VTE content.
- Cyber Challenge being used DoD-wide.
- DoD agency CIOs reporting of International Cyber Defense Workshop (ICDW)-like training exercises, enhancing the cybersecurity skills of personnel.