Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Office of the Secretary Of Defense	Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
Total Program Element	10.313	10.933	8.940	8.876	-	8.876	9.594	10.188	10.319	10.518	Continuing	Continuing
140: *Information Systems Security Program*	10.313	10.933	8.940	8.876	-	8.876	9.594	10.188	10.319	10.518	Continuing	Continuing

A. Mission Description and Budget Item Justification

The DoD CIO Information Systems Security Program (ISSP) provides for focused research, development, testing and integration of technology and technical solutions critical to the Defense Cybersecurity and Information Assurance Program 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/Instructions 8500, 8510, 8520, 8530, and 8540. This program is funded under Budget activity 7, Operational System Development because it integrates technology and technical solutions to the Defense Information Assurance Program.

ISSP RDT&E funds support the DoD CIO and its mission partners on architecting, engineering, and technical matters for developing governance processes and structures; on evolving and enabling a more integrated and synchronized Joint Information Environment that will leverage a single and converged joint enterprise IT platform; on the continued development of the U.S. Government's ability to prevent and defend against adversarial and/or commercial information and communications technology supply-chain attacks on its mission critical systems, networks, and devices; on improving oversight of the life-cycle management of cybersecurity risks; and on the integration of cybersecurity standards, methods, and procedures across the DoD for a more robust and resilient cybersecurity posture.

B. Program Change Summary ($ in Millions)	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Previous President's Budget	11.288	8.957	9.148	-	9.148
Current President's Budget	10.933	8.940	8.876	-	8.876
Total Adjustments	-0.355	-0.017	-0.272	-	-0.272
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.351	-			
• Program Adjustments	-0.004	-	-0.031	-	-0.031
• FFRDC Reduction	-	-0.017	-	-	-
• Efficiency Reduction	-	-	-0.182	-	-0.182
• Economic Assumptions	-	-	-0.059	-	-0.059

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Office of the Secretary Of Defense	Date: February 2016
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*

Change Summary Explanation

FY 2015: SIBR/STTR reduction -0.351 million, Program Adjustment -0.004 million.

FY 2016: FFRDC Reduction -0.017 million.

FY 2017: Efficiency Adjustment -0.182 million, Economic Assumption -0.059 Million, Program Adjustment -0.031 million.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense			Date: February 2016
Appropriation/Budget Activity 0400 / 7	R-1 Program Element (Number/Name) PE 0303140D8Z / *Information Systems Security Program*	Project (Number/Name) 140 / *Information Systems Security Program*	

COST ($ in Millions)	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
140: *Information Systems Security Program*	10.313	10.933	8.940	8.876	-	8.876	9.594	10.188	10.319	10.518	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The DoD CIO Information Systems Security Program (ISSP) provides for focused research, development, testing and integration of technology and technical solutions critical to the Defense Cybersecurity and Information Assurance Program 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/Instructions 8510, 8530 and 8540. This program is funded under Budget activity 7, Operational System Development because it integrates technology and technical solutions to the Defense Information Assurance Program.

ISSP RDT&E funds support the DoD CIO and its mission partners on architecting, engineering, and technical matters for developing governance processes and structures; on evolving and enabling a more integrated and synchronized Joint Information Environment that will leverage a single and converged joint enterprise IT platform; on the continued development of the U.S. Government's ability to prevent and defend against commercial information and communications technology supply-chain attacks on its mission critical systems, networks, and devices; on improving oversight of the life-cycle management of cybersecurity risks; and on the integration of cybersecurity standards, methods, and procedures across the DoD for a more robust and resilient cybersecurity posture.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
Title: Information Systems Security Program Plans and Accomplishments	10.933	8.940	8.876
FY 2015 Accomplishments: Continued support for, and development of, a single security architecture for: evolving the Joint Information Environment (JIE) and the JIE Regional Security Stacks (JRSS); to support the migration strategy and implementation plan for moving from the current construct to the JRSS framework; for data center and other critical mission infrastructure protection; for key technology insertions as needed; and the respective supporting cybersecurity policies and strategies. • Continued development and implementation of policies, strategies, and architectures for successful computer network defenses and operations in the event of large-scale cyber incidents by sophisticated cyber adversaries. Includes cybersecurity exercises, cyber incident response, computer network defense operations, resiliency, and outreach and engagement with mission partners as required. • Conducted research and analyses regarding security and potential threats to the Global Positioning System (GPS) and Positioning, Navigation, and Timing (PNT), the GPS Master Control Station analyses; and GPS Legacy Software Integrity.			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
• Conducted research to develop means of assessing and prioritizing supply-chain threats and responses, for training regarding threats and risks, and for program protection plans to address supply-chain risks -- to help ensure implementation of consistent protection practices from supply chain exploitation and attack within/by individual procurements of materiel and services on which the DoD systems, networks, and missions depend. Also continued development of an overarching international standard, and provide enhancements to integrate a family of existing standards, for improving supply-chain-risk-management practices. • Supported development and implementation of more robust governance mechanisms, including organizational policy documents that provide technical guidance and direction to the U.S. Government cross domain community, to minimize supply chain risks across the DoD components and activities. This included development of a Mission-Essential-elements-of-Information (MEI) framework to identify and investigate international cybersecurity policies, and practices that impact the abilities of US Forces to engage in both peacetime and in conflict scenarios, in collaboration with mission partners & non-governmental partners... • Continued to develop and publish supportive standards, guidance, and processes on the web-based Knowledge Service, for the continual reauthorization and cyber strengthening of information systems, and in satisfaction of requirements mandated by OMB Circular A-130. Continued software development and support to facilitate Defense Knowledge Service requirements and data updates. • Continued to support key acquisition programs-of-record (i.e., Major Automated Information Systems; Major Defense Acquisition Programs, and other special interest developmental and acquisition activities) to drive the development and implementation of more effective cybersecurity strategies, risk management plans, and processes. Included detailed analyses of Cybersecurity, Supply-Chain-Risk-Management, and Program-Protection-Plan artifacts in support of high risk programs In collaboration with OUSD/AT&L, continued development of a capability-based adversary cyber threat model for use in requirements and acquisition, to help insure realistic (cost effective) requirements for high risk programs. • Supported analysis to develop means for improving mission assurance, mitigation analyses, and vulnerability detection via hardware and software testing, and to help insure acquisitions are better integrated with informed threat prospects. • Provided for technical support for requirements of the Federal Risk and Authorization Management Program (FEDRAMP) for Cloud computing services, and for developing requisite security requirements -- policies, programs, & pilots -- for all wireless and mobile devices (including commercial) being deployed Department-wide. Continued implementation and oversight of the policies and capabilities to support the DoD Cloud and mobile device strategies and roadmaps. Develop, publish, and refine DoD			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
mobility strategy, and processes for use of commercial Cloud providers. Develop Cloud computing security guidance that details cybersecurity guidance and procedures for use by potential commercial Cloud service providers.			
FY 2016 Plans: • Continue to develop and provide required engineering support for critical architectures, to include the Joint Information Environment, C4I tactical networks, and for coalition and other mission partners. Continue to develop, refine, and implement a Joint Information Environment single security architecture strategy, and the related strategic metrics and enhanced analytical capabilities. • Continue to develop and implement strategies for successful defenses and operations in the event of sophisticated cyber adversaries and large-scale cyber incidents. • Continue to research to develop means of assessing and prioritizing supply-chain threats and responses, for training regarding threats and risks, and for program protection plans to address supply-chain risks, to help ensure implementation of consistent protection practices from supply chain exploitation and attack within/by individual procurements of materiel and services on which the DoD systems, networks, and missions depend.. • Continue development and implementation of a more robust governance mechanism to minimize supply chain risks across the DoD components and activities, and to develop an overarching international standard, or an improved integrated family of existing standards, for improving supply-chain-risk-management. • Continue to develop the means for improved mission assurance, mitigation analyses, and vulnerability detection via hardware and software testing, and for acquisitions that are better integrated with informed threat prospects. • Continue to develop and publish supportive standards, guidance, and processes on the web-based Knowledge Service, for the continual reauthorization and cyber strengthening of information systems, and in satisfaction of requirements mandated by OMB Circular A-130. • Continue to support key acquisition programs-of-record (i.e., Major Automated Information Systems; Major Defense Acquisition Programs, and other special interest developmental and acquisition activities) to drive the development and implementation of more effective cybersecurity strategies, risk management plans, and processes. • Continue to develop, publish, and refine DoD mobility strategy, and processes for use of commercial Cloud providers; to develop Cloud computing security guidance that details cybersecurity guidance and procedures for use by potential commercial Cloud			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
service providers, and continued oversight of policies and capabilities to support comprehensive cybersecurity capability for the Joint Information Environment (JIE), including the DoD Cloud and mobile device strategies and roadmaps. ***FY 2017 Plans:*** • Continue to develop and provide required engineering support for critical architectures, to include the Joint Information Environment, C4I tactical networks, and for coalition and other mission partners. Continue to develop, refine, and implement a Joint Information Environment single security architecture strategy, and the related strategic metrics and enhanced analytical capabilities. • Continue to develop and implement strategies for successful defenses and operations in the event of sophisticated cyber adversaries and large-scale cyber incidents. • Continue to research to develop means of assessing and prioritizing supply-chain threats and responses, for training regarding threats and risks, and for program protection plans to address supply-chain risks, to help ensure implementation of consistent protection practices from supply chain exploitation and attack within/by individual procurements of materiel and services on which the DoD systems, networks, and missions depend.. • Continue development and implementation of a more robust governance mechanism to minimize supply chain risks across the DoD components and activities, and to develop an overarching international standard, or an improved integrated family of existing standards, for improving supply-chain-risk-management. • Continue to develop the means for improved mission assurance, mitigation analyses, and vulnerability detection via hardware and software testing, and for acquisitions that are better integrated with informed threat prospects. • Continue to develop and publish supportive standards, guidance, and processes on the web-based Knowledge Service, for the continual reauthorization and cyber strengthening of information systems, and in satisfaction of requirements mandated by OMB Circular A-130. • Continue to support key acquisition programs-of-record (i.e., Major Automated Information Systems; Major Defense Acquisition Programs, and other special interest developmental and acquisition activities) to drive the development and implementation of more effective cybersecurity strategies, risk management plans, and processes. • Continue to develop, publish, and refine DoD mobility strategy, and processes for use of commercial Cloud providers; to develop Cloud computing security guidance that details cybersecurity guidance and procedures for use by potential commercial Cloud			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
service providers, and continued oversight of policies and capabilities to support comprehensive cybersecurity capability for the Joint Information Environment (JIE), including the DoD Cloud and mobile device strategies and roadmaps.			
Accomplishments/Planned Programs Subtotals	10.933	8.940	8.876

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• 0303140D8Z O&M DW: *Information System Security Program*	10.992	13.490	11.321	-	11.321	11.644	11.307	11.459	11.687	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

- Annual FISMA metrics
- Evolving JIE cybersecurity metrics

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Studies Analysis	Various	Various : Various	0.795	1.057	Jul 2015	0.840	Jul 2016	0.861	Jul 2017	-		0.861	Continuing	Continuing	Continuing
Technical Engineering Services	Various	Various : Various	5.216	5.305	Jul 2015	4.486	Jul 2016	4.289	Jul 2017	-		4.289	Continuing	Continuing	Continuing
Services Supporty	Various	Various : Various	0.099	0.105	Jul 2015	0.083	Jul 2016	0.086	Jul 2017	-		0.086	Continuing	Continuing	Continuing
		Subtotal	6.110	6.467		5.409		5.236		-		5.236	-	-	-

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Support	Various	Various : Various	0.200	0.212	Jul 2015	0.168	Jul 2016	0.173	Jul 2017	-		0.173	Continuing	Continuing	Continuing
Engineering Support	FFRDC	Various : Various	2.910	3.092	Jul 2015	2.440	Jul 2016	2.520	Jul 2017	-		2.520	Continuing	Continuing	Continuing
R&D Support	Various	Various : Various	1.093	1.162	Jul 2015	0.923	Jul 2016	0.947	Jul 2017	-		0.947	Continuing	Continuing	Continuing
		Subtotal	4.203	4.466		3.531		3.640		-		3.640	-	-	-

	Prior Years	FY 2015		FY 2016		FY 2017 Base		FY 2017 OCO		FY 2017 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	10.313	10.933		8.940		8.876		-		8.876	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Office of the Secretary Of Defense			Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*	

R4

PE: 0303140D8Z/ Information Systems Security Program

Funding supports 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.

	10/1/2014	10/1/2015	10/1/2016	10/1/2017	10/1/2018	10/1/2019	10/1/2020	10/1/2021
FY2014 Program Execution								
FY2015 Program Execution								
FY2016 Program Execution								
FY2017 Program Execution								
FY2018 Program Execution								
FY2019 Program Execution								
FY2020 Program Execution								

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Office of the Secretary Of Defense		Date: February 2016
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140D8Z / *Information Systems Security Program*	**Project (Number/Name)** 140 / *Information Systems Security Program*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
FY15 Project Execution	1	2015	4	2016
FY16 Project Execution	1	2016	4	2017
FY17 Project Execution	1	2017	4	2018
FY18 Project Execution	1	2018	4	2019
FY 19 Project Execution	1	2019	4	2020
FY 20 Project Execution	1	2020	4	2021