Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Office of the Secretary Of Defense	Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
Total Program Element	21.246	8.649	8.876	9.415	-	9.415	9.966	10.067	10.262	10.491	Continuing	Continuing
140: *Information Systems Security Program*	21.246	8.649	8.876	9.415	-	9.415	9.966	10.067	10.262	10.491	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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	8.940	8.876	9.594	-	9.594
Current President's Budget	8.649	8.876	9.415	-	9.415
Total Adjustments	-0.291	0.000	-0.179	-	-0.179
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.291	-			
• SRRB Efficiency	-	-	-0.332	-	-0.332
• Program Adjustment	-	-	0.153	-	0.153

Change Summary Explanation

FY 2016: SIBR Adjustment -0.253 million, STTR Adjustment -0.038 million.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Office of the Secretary Of Defense	Date: May 2017
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*

FY 2017: No change.

FY 2018: SRRB Efficiency -0.332 million, Program adjustment 0.153 million.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
140: *Information Systems Security Program*	21.246	8.649	8.876	9.415	-	9.415	9.966	10.067	10.262	10.491	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 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 (JIE) to provide the means for more integrated information sharing and collaboration that also endeavors to close identified gaps across all mission areas with a shared network of core enterprise services; 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. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Information Systems Security Program Plans and Accomplishments	8.649	8.876	9.415
FY 2016 Accomplishments: • Developed required engineering support concepts 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. • Developed strategies for successful defenses and operations in the event of sophisticated cyber adversaries and large-scale cyber incidents, analyses & development of metrics focused on the cybersecurity domain, on cybersecurity scorecard and automation, analyses to support policy development and refinement, oversight, and formulation of programmatic advice, and analyses to support various collaborative advisory and governance bodies. • Researched 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			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense		Date: May 2017
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 2016	FY 2017	FY 2018
from supply chain exploitation and attack within/by individual procurements of materiel and services on which the DoD systems, networks, and missions depend.. • Developed paradigm of threat-based system-security-engineering, including generation of critical design artifacts (threat analyses, risk analyses, system-of- system-security architectures), and with demonstrated applications to space systems and mission partner environment (MPE). • Continued to develop 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. • Continued developing 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. • Developed and published 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. • Supported 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. • Developed, published, and refined 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 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.			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense		Date: May 2017
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 2016	FY 2017	FY 2018
• 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 threat-based system-security-engineering efforts and development of critical design artifacts (threat analyses, risk analyses, system-of- system-security architectures), having demonstrated applications to space systems and mission partner environment (MPE). • 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 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 roadmap ***FY 2018 Plans:***			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense		Date: May 2017
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 2016	FY 2017	FY 2018
• 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 threat-based system-security-engineering efforts and development of critical design artifacts (threat analyses, risk analyses, system-of- system-security architectures), having demonstrated applications to space systems and mission partner environment (MPE). • 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: FY 2018 Office of the Secretary Of Defense		Date: May 2017
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 2016	FY 2017	FY 2018
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	8.649	8.876	9.415

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• 0303140D8Z O&M DW: *Information System Security Program*	11.490	11.321	11.867	-	11.867	10.474	10.590	10.809	11.033	Continuing	Continuing

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

- Annual FISMA metrics
- Evolving JIE cybersecurity metrics