Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Defense Information Systems Agency	Date: February 2018
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*

COST ($ in Millions)	Prior Years	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
Total Program Element	-	0.000	0.000	19.611	-	19.611	12.596	12.904	13.122	13.770	Continuing	Continuing
IA3: *Information Systems Security Program*	-	0.000	0.000	19.611	-	19.611	12.596	12.904	13.122	13.770	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) mission focuses on developing Department of Defense (DoD) enterprise solutions to Combatant Commands, Services, and Defense-wide agencies to ensure critical mission execution in the face of cyber attacks. The ISSP ensures that, the network, the computing centers, and core enterprise services will evolve to better support a joint cybersecurity/information assurance model that has common enterprise-scale perimeter defenses and will support a broad range of sharing policies from completely unclassified to tightly-held within a classified community. The ISSP will test and develop active-active defensive capabilities; test and integrate software defined networking and orchestration closed-loop security; perform research, development and engineering of emerging cyber situational awareness technologies; harden the network by providing architecture support, systems engineering and analytical functions for Endpoint and Perimeter defense capabilities; cyber IT infrastructure and automation support to deploy enterprise-wide next generation identity technologies; and develop and evolve an integrated cyber domain security workforce to be on the leading edge of defensive capabilities.

B. Program Change Summary ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Previous President's Budget	0.000	0.000	4.500	-	4.500
Current President's Budget	0.000	0.000	19.611	-	19.611
Total Adjustments	0.000	0.000	15.111	-	15.111
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Other Adjustments	-	-	15.111	-	15.111

Change Summary Explanation

The increase of +$15.111 in FY 2019 is attributed to additional engineering and software expertise in support of the User Activity Monitoring (UAM) capability in countering insider threats at nine Combatant Commands; engineering and software expertise necessary to develop, test, and deploy the Automated Patch Management (APM) Proof of Concept and associated platform.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Defense Information Systems Agency			Date: February 2018
Appropriation/Budget Activity 0400 / 7	R-1 Program Element (Number/Name) PE 0303140K / *Information Systems Security Program*	Project (Number/Name) IA3 / *Information Systems Security Program*	

COST ($ in Millions)	Prior Years	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
IA3: *Information Systems Security Program*	-	0.000	0.000	19.611	-	19.611	12.596	12.904	13.122	13.770	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) mission focuses on developing Department of Defense (DoD) enterprise solutions to Combatant Commands, Services, and Defense-wide agencies to ensure critical mission execution in the face of cyber attacks. The ISSP ensures that, the network, the computing centers, and core enterprise services will evolve to better support a joint cybersecurity/information assurance model that has common enterprise-scale perimeter defenses and will support a broad range of sharing policies from completely unclassified to tightly-held within a classified community. The ISSP will test and develop active-active defensive capabilities; test and integrate software defined networking and orchestration closed-loop security; perform research, development and engineering of emerging cyber situational awareness technologies; harden the network by providing architecture support, systems engineering and analytical functions for Endpoint and Perimeter defense capabilities; cyber IT infrastructure and automation support to deploy enterprise-wide next generation identity technologies; and develop and evolve an integrated cyber domain security workforce to be on the leading edge of defensive capabilities.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Title: Zero-Day Network Defense Email Capability ***Description:*** Zero-Day Network Defence (ZND) Email Capability Technology Assessment/Evaluation for Tech Refresh. ***FY 2019 Plans:*** Conduct Technology Assessment/Evaluation in support of Zero-Day Network Defense (ZND) Email Tech Refresh. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase +$4.500 from FY 2018 for FY 2019 is for the technology evaluation in support of tech refresh of the Zero Day Net Defense (ZND) email capability on the Non-classified Internet Protocol Router Network (NIPRNet). This increase supports research and engineering solutions for enhanced malware analysis, preventative spear-phishing and perimeter attacks within the DoDIN, design of layered defenses against adversary Tactics, Techniques, and Procedures (TTPs) and testing of automated machine to machine processes of cyber situational awareness at the five email gateways.	0.000	-	4.500
Title: DoD Cyber Security Range (CSR) ***Description:*** The DoD Cyber Security Range (CSR) provides a multi-classification level, operationally realistic, DoDIN representative, cyber security environment to sustain and enhance the professional development of the DoD cyber security workforce.	0.000	-	1.811

Exhibit R-2A, RDT&E Project Justification: PB 2019 Defense Information Systems Agency		Date: February 2018
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*	**Project (Number/Name)** IA3 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
FY 2019 Plans: Continue providing the IA Range platform to test new Cybersecurity efforts using the CS Range; Increase capability to leverage CS Range for training and capstone events; Increase capability for remote access to CS Range for testing, training and exercises. Implement Joint Regional Security Stacks (JRSS) Cloud Learning Environment improvements, JRSS Management System (JMS) Enhancements, and replicate the tactical network boundaries of the four services. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase of $1.811 from FY 2018 to FY 2019 is due to the additional testing and simulation requirements for the operational networks within the Cybersecurity Range, including exploitation, evaluation of new capabilities, immersive training, tactics and techniques, procedures development and validation, system interoperability and integration testing, and certification and accreditation.			
Title: Endpoint Security Solutions (ESS) ***Description:*** Description: Endpoint Security Solutions (ESS) provides counters exploitation and destructive malware, contain exploited threats, and make indicators of attack/compromise visible to the operator; fully supports friendly forces operating in contested cyber environments. Provides Asset Inventory Management Modules (AIMM) to provide near-real time situational awareness of devices. Provides Digital Policy Management System (DPMS) to facilitate development and maintenance of Cybersecurity/Information Assurance Standards. Provides Assured Compliance Assessment Solution (ACAS) to assess the configuration compliance of networks and systems against DoD and all known vulnerabilities. ***FY 2019 Plans:*** Provide software licensing necessary to perform the Automated Patch Management (APM) Proof of Concept, technical expertise necessary to deploy this APM solution, and additional infrastructure investment to provide an updated platform for the APM effort to be successful. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase of +$3.000 from FY 2018 to FY 2019 is attributable to the additional requirements for software licensing to conduct the Automated Patch Management (APM) Proof of Concept.	0.000	-	3.000
Title: Cyber HQs Support ***Description:*** Preserves User Activity Monitoring (UAM) capability in countering insider threats at nine Combatant Commands. ***FY 2019 Plans:***	0.000	-	10.300

Exhibit R-2A, RDT&E Project Justification: PB 2019 Defense Information Systems Agency		Date: February 2018
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*	**Project (Number/Name)** IA3 / *Information Systems Security Program*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019
Perform engineering and provide software licensing/maintenance in support of the User Activity Monitoring (UAM) capability in countering insider threats at nine Combatant Commands. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The increase of +$10.300 from FY 2018 for FY 2019 is attributable to additional engineering contract support and software licensing/maintenance support for the User Activity Monitoring (UAM) capability in countering insider threats at nine Combatant Commands.			
Accomplishments/Planned Programs Subtotals	0.000	-	19.611

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Conduct Technology Assessment/Evaluation in support of Zero-Day Network Defense (ZND) Email Tech Refresh. Performance objectives include 60% of Defense Enterprise Email (DEE) Mailboxes protected, 0% bypassed emails, and capability to handle up to 43% unique attachments to total threats detected.

Continue providing the IA Range platform to test new Cybersecurity efforts using the CS Range; Increase capability to leverage CS Range for training and capstone events; Increase capability for remote access to CS Range for testing, training and exercises. Implement Joint Regional Security Stacks (JRSS) Cloud Learning Environment improvements, JRSS Management System (JMS) Enhancements, and replicate the tactical network boundaries of the four services. Annual objectives include 15 test and evaluation events, 9 training events, and support of 5 exercise events.

Provide engineering expertise and software licensing/maintenance in support of the User Activity Monitoring (UAM) capability in countering insider threats at nine CCMDs (USSOCOM, USAFRICOM, USCENTCOM, USEUCOM, USNORTHCOM, USPACOM, USSOUTHCOM, USSTRATCOM, and USTRANSCOM).

Acquire software licensing necessary to perform the Automated Patch Management (APM) Proof of Concept, technical expertise necessary to deploy this APM solution, and infrastructure investment to provide an updated platform for the APM effort to be successful.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Defense Information Systems Agency			Date: February 2018
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*	**Project (Number/Name)** IA3 / *Information Systems Security Program*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Need this info from RMO office	C/CPFF	TBD : TBD	-	-		-		-		-		-	Continuing	Continuing	-
		Subtotal	-	-		-		-		-		-	Continuing	Continuing	N/A

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
ZND Technology Assessment/Evaluation for email capability Tech Refresh	C/FFP	TBD : TBD	-	-		-		4.500	Feb 2019	-		4.500	Continuing	Continuing	-
DoD Cyber Security Range (CSR) Virtual Training Environment	C/FFP	ManTech : Fairfax, VA	-	-		-		1.198	Feb 2019	-		1.198	Continuing	Continuing	-
DoD Cyber Security Range (CSR) Virtual Training Environment - Re-compete	C/FFP	TBD : TBD	-	-		-		0.483	Jun 2019	-		0.483	Continuing	Continuing	-
DoD Endpoint Security Solutions (ESS)	C/FFP	TBD : TBD	-	-		-		3.000	Jan 2019	-		3.000	Continuing	Continuing	-
Cyber HQs Support	C/FFP	TBD : TBD	-	-		-		10.300	Jan 2019	-		10.300	Continuing	Continuing	-
Joint Information Operations Range (JIOR) Connection	C/FFP	TBD : TBD	-	-		-		0.130	Jan 2019	-		0.130	Continuing	Continuing	-
		Subtotal	-	-		-		19.611		-		19.611	Continuing	Continuing	N/A

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	-		0.000		19.611		-		19.611	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Defense Information Systems Agency		Date: February 2018
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*	**Project (Number/Name)** IA3 / *Information Systems Security Program*

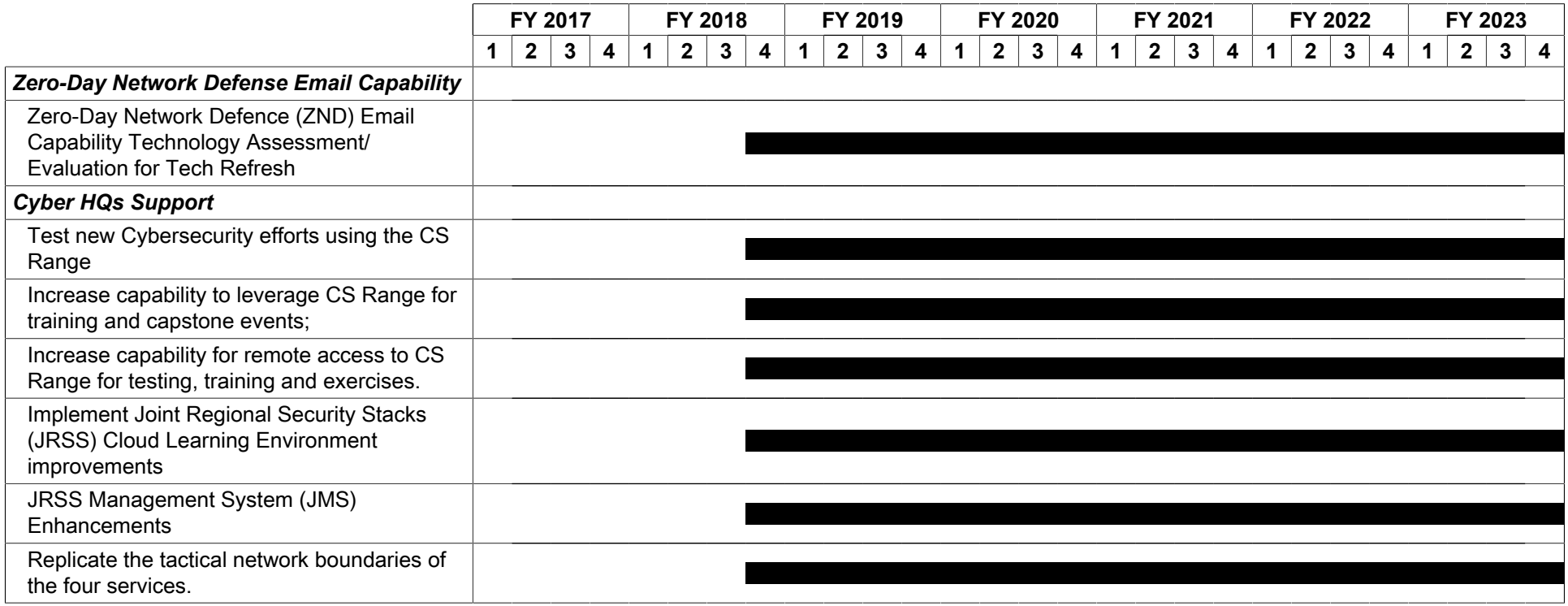

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Defense Information Systems Agency		Date: February 2018
Appropriation/Budget Activity 0400 / 7	**R-1 Program Element (Number/Name)** PE 0303140K / *Information Systems Security Program*	**Project (Number/Name)** IA3 / *Information Systems Security Program*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Zero-Day Network Defense Email Capability				
Zero-Day Network Defence (ZND) Email Capability Technology Assessment/ Evaluation for Tech Refresh	4	2018	4	2023
Cyber HQs Support				
Test new Cybersecurity efforts using the CS Range	4	2018	4	2023
Increase capability to leverage CS Range for training and capstone events;	4	2018	4	2023
Increase capability for remote access to CS Range for testing, training and exercises.	4	2018	4	2023
Implement Joint Regional Security Stacks (JRSS) Cloud Learning Environment improvements	4	2018	4	2023
JRSS Management System (JMS) Enhancements	4	2018	4	2023
Replicate the tactical network boundaries of the four services.	4	2018	4	2023