Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Defense Information Systems Agency	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	0.000	42.262	40.398	8.922	-	8.922	6.485	7.222	9.065	9.109	Continuing	Continuing
IA3: *Information Systems Security Program*	0.000	42.262	40.398	8.922	-	8.922	6.485	7.222	9.065	9.109	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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	19.611	42.796	12.904	-	12.904
Current President's Budget	42.262	40.398	8.922	-	8.922
Total Adjustments	22.651	-2.398	-3.982	-	-3.982
• Congressional General Reductions	-	-2.398			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	22.717	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.066	-			
• Adjustment	-	-	-3.982	-	-3.982

Change Summary Explanation

The increase of +$22.651 in FY2019 reflects a transfer of funding to Small Business Innovation research (SBIR) and Small Business Technology Transfer (STTR) programs (-$0.066) and an increase of +$22.717 received through a congressional reprogramming action for Secure Application Development (DevSecOps) (+$4.500); Identity Credentialing and Access Management (ICAM) (+$12.200) and Zero Trust Architecture (ZTA) (+$6.000). DevSecOps is to develop integrated tools and standards that enable users and partners to develop, deploy, and operate applications in a security and flexible environment. ICAM will standardize

credentialing capabilities for secure access to mobile devices and ZTA implements the Department's security protocols by continuously verifying everyone within the network.

The decrease of -$2.398 in FY 2020 is attributable to the Congressional directed transfer of Sharkseer from NSA to DISA ($1.882) and a Congressional general reduction of -$4.280 for unjustified growth.

The decrease of -$3.982 in FY 2021 is due to an increase for Zero Trust Architecture (ZTA) to further develop the DoD architectures for Zero-Trust Architecture and lab development (+$2.462) and a decrease due to the elimination of the DISA Cybersecurity Information Assurance Range, to avoid duplication of effort with the CYBERCOM Range under development. Also a reduction to cyber innovation and "DWR".

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Information Systems Agency			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
IA3: *Information Systems Security Program*	0.000	42.262	40.398	8.922	-	8.922	6.485	7.222	9.065	9.109	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 2019	FY 2020	FY 2021
Title: Zero-Day Network Defense Email Capability ***Description:*** Zero-Day Network Defense (ZND) Email Capability Technology Assessment/Evaluation for Tech Refresh.	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. ***FY 2020 Plans:*** Continue providing the Cybersecurity (CS) / Information Assurance (IA) Range platform to test new Cybersecurity efforts using the CS Range; Continue to support capability to leverage CS Range for training and capstone events; Support 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 2020 to FY 2021 Increase/Decrease Statement:***	1.351	1.337	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Information Systems Agency		Date: February 2020
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 2019	FY 2020	FY 2021
The decrease of -$1.337 between FY 2020 and FY 2021 is due to the elimination of the DISA Cybersecurity Information Assurance Range to avoid duplication of effort with the CYBERCOM Range under development and apart of the "DWR".			
Title: Endpoint Security Solutions (ESS) ***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.	3.000	-	-
Title: Cyber HQs Support ***Description:*** Preserves User Activity Monitoring (UAM) capability in countering insider threats at nine Combatant Commands.	10.300	-	-
Title: Cyber Innovation and Technology ***Description:*** Provide research and development, conduct technology assessments, rapidly produce prototypes using commercial solutions, validate assumptions, and provide empirical data to drive real time enterprise solutions and decisions in assisting DoD requirement owners for enterprise fielding of innovative gap fillers to address cyber capabilities and militarization of commercial information assurance capabilities tactical edge. All project undertaken directly increase information sharing capabilities and assure C2 functionality against a common operating picture. The program will leverage its robust IT infrastructure to develop small prototypes to find cost saving initiatives across the DoD Information Network (DODIN) in an effort to provide the DoD with faster more reliable communications capabilities. These solutions will look to provide enhanced warfighting technology and research development programs improving the protection, survivability, mobility and combat effectiveness of the DoD. ***FY 2020 Plans:*** Assess, test, and prototype DoDCAR (DoD Cybersecurity Analysis and Review processes), including portfolio management against threat coverage and analyses of advisory behaviors within DoD Networks. Perform an assessment of Blockchain commercial capabilities, evaluating them for suitability to enhance enterprise level services for DoD entities. ***FY 2021 Plans:*** Continued assessment, testing, prototype improvement and implementation of DoDCAR (DoD Cybersecurity Analysis and Review processes. This includes portfolio management against threat coverage and the execution of deeper analyses of advisory behaviors within DoD Networks. ***FY 2020 to FY 2021 Increase/Decrease Statement:***	0.411	1.179	0.464

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Information Systems Agency		Date: February 2020
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 2019	FY 2020	FY 2021
The decrease of -$0.715 from FY 2020 to FY 2021 is due to a reduction in the scope of Cyber Innovation & Technology efforts, specifically early completion of the Blockchain assessment in FY 2020.			
Title: Identity, Credential, and Access Management (ICAM) ***Description:*** Develop and deploy Identity, Credential, and Access Management (ICAM) efforts associated with automated account provisioning and auditability and federalized authentication services that support credentials for DoD and non-DoD personnel. ***FY 2020 Plans:*** Conduct the Master User Record (MUR) pathfinder effort and several Automated Account Provisioning (AAP) use-case Pilots. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The decrease of -$30.000 from FY 2020 to FY 2021 is due to completion of one-time funding of Master User Record (MUR) pathfinder effort and several Automated Account Provisioning (AAP) use-case pilots.	12.200	30.000	-
Title: Sharkseer ***Description:*** SHARKSEER is a critical component of the Cyber Kill Chain that uniquely enhances the defensive posture of the Department of Defense Information Network (DoDIN) by assisting us with mitigating unknown (zero-day) cyber threats in near-real time utilizing orchestration. SHARKSEERs primary mission is to detect and mitigate Zero-Days and Advanced Persistent Threats (APTs) at DoDIN IAPs. SHARKSEER also provides Malware Analytics, Deep Packet Analysis, Global Threat Intelligence, and Cyber Threat Indicator (CTI) sharing to Federal Agencies, Military Departments, and Services. ***FY 2020 Plans:*** Research and develop next generation advance architecture to provide a more scalable system that can also more effectively respond to unknown cyber security threats that traverse the Department of Defense Information Networks (DoDIN). ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The decrease of -$1.882 from FY 2020 to FY 2021 is due to completion of next generation advance architecture.	-	1.882	-
Title: Zero Trust Architecture (ZTA) ***Description:*** Will develop, test, and evaluate the technologies required for the implementation of ZTA. ***FY 2021 Plans:*** To develop, test, and evaluate technologies, identify critical applications on SIPR that are required to improve security, and analyze backbone design, gateway, and mobility infrastructure for necessary improvements. ***FY 2020 to FY 2021 Increase/Decrease Statement:***	6.000	-	2.462

Exhibit R-2A, RDT&E Project Justification: PB 2021 Defense Information Systems Agency		Date: February 2020
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 2019	FY 2020	FY 2021
The increase of $2.462 between FY 2020 and FY 2021 will further the DoD architectures for Zero-Trust Architecture (ZTA) and lab development. The labs purpose is to replicate the DoD infrastructure in order to validate architectures. Funding will be utilized for lab improvements to test and verify vendor equipment and contractor labor support.			
Title: Secure Application Development (DevSecOps) Program ***Description:*** Will provide an enterprise capability for an automated DevSecOps platform that programs can use to rapidly and automatically build, accredit, secure, test, deploy, monitor, and protect newly developed applications. ***FY 2020 Plans:*** Develops integrated tools and standards that enable users and partners to develop, deploy, and operate applications in a secure and flexible environment. ***FY 2021 Plans:*** Develops integrated tools and standards that enable users and partners to develop, deploy, and operate applications in a secure and flexible environment. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** The decrease of -$.004 from FY 2020 to FY 2021 is due to an non-pay non-fuel inflation adjustment.	4.500	6.000	5.996
Accomplishments/Planned Programs Subtotals	42.262	40.398	8.922

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• O&M, DW: *PE 0303140K*	0.000	0.000	56.974	0.000	56.974	59.237	57.545	56.380	58.837	Continuing	Continuing
• Procurement, DW: *PE 0303140K*	0.000	0.000	4.160	0.000	4.160	2.214	4.258	6.300	6.432	Continuing	Continuing

Remarks

N/A

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Defense Information Systems Agency			Date: February 2020
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*	

Support ($ in Millions)				FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
ZND Technology Assessment/Evaluation for email capability Tech Refresh	C/FFP	ASRC Federal : Beltsville, MD	-	16.705	Feb 2019	-		-		-		-	0.000	16.705	-
DoD Cyber Security Range (CSR) Virtual Training Environment	C/FFP	ManTech : Fairfax, VA	-	2.198	Feb 2019	-		-		-		-	0.000	2.198	-
DoD Cyber Security Range (CSR) Virtual Training Environment - Re-compete	C/FFP	ManTech : Fairfax, VA	-	0.476	Jun 2019	1.207	Sep 2020	-		-		-	Continuing	Continuing	-
DoD Endpoint Security Solutions (ESS)	C/FFP	TBD : TBD	-	-		-		-		-		-	0.000	0.000	-
Cyber HQs Support	C/FFP	Bylight : Fort Meade, MD	-	18.705	Jan 2019	-		-		-		-	0.000	18.705	-
Joint Information Operations Range (JIOR) Connection	C/FFP	ManTech : Stafford, VA	-	0.130	Jan 2019	0.130	Sep 2020	-		-		-	Continuing	Continuing	-
DISA EA Model Development for Cyber Security and Network Technical Domains, DODCAR Cyber Analysis Tool Development	C/FFP	Various : Various	-	4.048		0.459	Jan 2020	0.464	Jan 2021	-		0.464	Continuing	Continuing	-
Deployment of Blockchain and Next Generation Identity	C/FFP	TBD : TBD	-	-		6.000	Jan 2020	1.494	Jan 2021	-		1.494	Continuing	Continuing	-
Cyber Innovation and Technology	C/FFP	TBD : TBD	-	-		5.000	Mar 2020	-		-		-	Continuing	Continuing	-
Identity, Credential, and Access Management (ICAM)	C/FFP	TBD : TBD	-	-		27.602	Mar 2020	-		-		-	Continuing	Continuing	-
Sharkseeker	C/FFP	TBD : TBD	-	-		-		4.500		-		4.500	Continuing	Continuing	-
Zero Trust Architecture (ZTA)	C/FFP	TBD : TBD	-	-		-		2.464		-		2.464	Continuing	Continuing	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Defense Information Systems Agency		Date: February 2020
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*

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	-	42.262		40.398		8.922		-		8.922	Continuing	Continuing	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	42.262		40.398		8.922		-		8.922	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Defense Information Systems Agency			Date: February 2020
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*	

	FY 2012				FY 2013				FY 2014				FY 2015				FY 2016				FY 2017				FY 2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Zero-Day Network Defense Email Capability																												
Zero-Day Network Defence (ZND) Email Capability Technology Assessment/ Evaluation for Tech Refresh																												■
Cyber HQs Support																												
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																												■
Replicate the tactical network boundaries of the four services.																												■
Architecture and Model development																												
DODCAR WG Support																												
Innovation and Technology																												
Block Chain Cyber Innovation Technology Assessment																												
Next Gen Identity Tool Suite Cyber Innovation Technology Assessment																												
Zero Trust Architecture (ZTA)																												
Develop, test, and evaluate the technologies																												

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Defense Information Systems Agency		Date: February 2020
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*

	FY 2012				FY 2013				FY 2014				FY 2015				FY 2016				FY 2017				FY 2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Sharkseer																												
To develop Sharkseer 2.0																												

	FY 2019				FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Zero-Day Network Defense Email Capability																												
Zero-Day Network Defence (ZND) Email Capability Technology Assessment/ Evaluation for Tech Refresh																												
Cyber HQs Support																												
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																												
Replicate the tactical network boundaries of the four services.																												
Architecture and Model development																												
DODCAR WG Support																												
Innovation and Technology																												

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Defense Information Systems Agency		Date: February 2020
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*

	FY 2019				FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Block Chain Cyber Innovation Technology Assessment																												
Next Gen Identity Tool Suite Cyber Innovation Technology Assessment																												
Zero Trust Architecture (ZTA)																												
Develop, test, and evaluate the technologies																												
Sharkseer																												
To develop Sharkseer 2.0																												

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Defense Information Systems Agency		Date: February 2020
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	2019
Cyber HQs Support				
Test new Cybersecurity efforts using the CS Range	4	2018	4	2019
Increase capability to leverage CS Range for training and capstone events;	4	2018	4	2019
Increase capability for remote access to CS Range for testing, training and exercises.	4	2018	4	2019
Implement Joint Regional Security Stacks (JRSS) Cloud Learning Environment improvements	4	2018	4	2019
JRSS Management System (JMS) Enhancements	4	2018	4	2019
Replicate the tactical network boundaries of the four services.	4	2018	4	2019
Architecture and Model development				
DODCAR WG Support	2	2020	3	2025
Innovation and Technology				
Block Chain Cyber Innovation Technology Assessment	3	2020	3	2024
Next Gen Identity Tool Suite Cyber Innovation Technology Assessment	3	2020	3	2024
Zero Trust Architecture (ZTA)				
Develop, test, and evaluate the technologies	4	2021	3	2025
Sharkseer				
To develop Sharkseer 2.0	4	2021	3	2025