Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army											Date: May 2021	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*							
COST ($ in Millions)	**Prior Years**	**FY 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
Total Program Element	-	25.710	28.270	15.720	-	15.720	-	-	-	-	-	-
491: *Information Assurance Development*	-	8.368	8.009	6.937	-	6.937	-	-	-	-	-	-
DV4: *Key Management Infrastructure (KMI)*	-	11.687	12.457	0.987	-	0.987	-	-	-	-	-	-
DV5: *Crypto Modernization (Crypto Mod)*	-	5.655	7.804	7.796	-	7.796	-	-	-	-	-	-

A. Mission Description and Budget Item Justification

The Information Systems Security Program funding line supports the Army Network Modernization Strategy LOE 1, Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy.

Project 491: Army CIO/G6 manages Project 491

Project 491: Information Assurance (IA) Development supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) Modernization and Key Management (KM) technologies within the Army. This including current and next generation encryption techniques, current and future Key Management Infrastructure (KMI) and technology migrations. This program provides oversight in developing policies, guidance, standard operating procedures and recommendations in integrating COMSEC and KM techniques into specific systems in support of securing the Army Tactical and Enterprise Networks. This entails architecture studies, system integration and testing, developing installation kits, and technological collaborations with NSA, DISA and other Services for enterprise and last mile implementations. The program assesses, develops and integrates Cyber Security (CS)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance (SPG) and the Army Modernization and Strategy Plan (AMSP).

IA Development funding implements and establishes functional and technical boundaries of cryptographic, key management and IA capabilities in coordination with the NSA, the DISA, and Joint Services, to secure National Security Systems (NSS), and National Security Information (NSI). Technical evaluations assess the security, operational effectiveness and network interoperability of advanced concept technologies to develop policies, standards, and fundamental building blocks for Army COMSEC capabilities that reduce the risk of future material solutions that could underperform and disrupt classified operations. Develop and publish the COMSEC Implementation Planning Guidance to identify, standardize, and govern the insertion of CS capabilities to bridge operational gaps and support the DoD and NSA mandated requirements to enhance network capacity while providing for secure information exchange of voice, video, and data in accordance with the Army Network Campaign Plan. This will be accomplished by interoperability evaluation, standards testing, and CS, System of System Network Vulnerability Assessments (SoS NVA) for Army Capability Sets for CS/COMSEC capabilities that provide protections for tactical and fixed infrastructure post, camp, and station networks.

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army	Date: May 2021
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140A *I Information Systems Security Program*

Project 491 FY 2022 Justification: This funding enables the continuation of oversight for the executions of the Army's COMSEC Modernization initiatives including major Advanced Cryptographic Capabilities (ACC) updates and replacements of existing devices and systems to meet NSA mandates. Continue to support the evaluation and testing of new technologies to support DoD Cryptographic Moderation 2 (CM2) Army implementations including Transmission Security (TRANSEC), EKMS to KMI migration and S-ICAN/ITN architecture future Capability Set developments. Support efforts to provide updated end-to-end, tactical-to-strategic COMSEC standardization and implementation guidance to meet Army's operational requirements. Continuous funding will enable the evaluations and maturity assessment of new COMSEC and key management capabilities developed by DoD joint KMI program for Army fielding to protect and strengthen the Army Network posture, with reduced cryptographic interoperability issues for both embedded and standalone systems. This funding also supports the risk reduction testing to document operational value of commercial products prior to insertion for Army use. Provide timely test and evaluate results to enable the Army to make sound investment strategic decisions and to reduce or eliminate duplications. Also supports efforts to update and develop policies to posture Army's operations to implement innovative cryptographic and key management tools and services. Perform System of System Network Vulnerability Assessments (SoS NVA) to provide protections for the Army Integrated Tactical Networks.

The Defensive Cyberspace Operations (DCO) program provides initial capabilities that enable passive and active cyberspace defense operations to preserve friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Big Data Pilot provides an advanced analytics capability capable of ingesting structured, semi-structured, and unstructured data from multiple data sources (e.g., Joint Regional Security Stacks (JRSS), intrusion detection systems, intrusion prevention systems, network device log files, trouble tickets, firewalls, proxies, web and applications server log files, etc) and proves situational awareness of cyberspace battlefield. It provides the computer network defense provider with common analytic platform which informs and reduces risk associated with future material solutions and forms a blueprint for future Big Data Analytics. Big Data (analysis-of-all DoD Information Network sensor data) provides two optimized and accredited clusters deployed in support of JRSS and Defense Research and Engineering Network (DREN) with a tools suite accessible to Cyber Mission Forces via secure remote access. The Army's DCO activities are a construct of active cyberspace defenses which provide synchronized, real-time capability to discover, detect, analyze, and mitigate threats to and vulnerability of DoD networks and systems.

Project DV4 & DV5: COMSEC is governed by the Chairman of the Joint Chiefs of Staff Instruction (CJCSA) 6510. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army communications systems are required to support modern cryptographic capabilities by implementing modern algorithms. These efforts are consistent with Strategic Planning Guidance (SPG). These funding lines support the Army Network Modernization Strategy LOE 1, Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy.

Project DV4: The Army Key Management Infrastructure (AKMI) is the Army's implementation of the National Security Agency (NSA) KMI ACAT IAM program, automating the functions of COMSEC electronic key management, control, planning, and distribution. AKMI supports the Army's ability to communicate and distribute Cryptographic data on the Army's tactical and strategic networks by limiting adversarial access to and reducing the vulnerability of, Army Command, Control, Communications, Computers, Cyber, Intelligence (C5I) systems. AKMI devices receive, store, manage, and transfer electronic key through the network to be loaded into communication devices such as radios and satellites to secure the network. Without this technology Warfighters are required to manually receive their cryptographic products by traveling to COMSEC account locations (which may not be co-located) and manually fill their devices.

Project DV4 FY 2022 Justification: This funding line supports COMSEC technologies within the Army with allocations for the following: $0.987M, Reprogrammable Single Chip Universal Encryptor (RESCUE) to create a secure, reprogrammable cryptographic engine in providing Cryptographic Modernized Capabilities including future Over

the Network Keying (OTNK) to Fill Devices and End Cryptographic Units (ECU)s. The RESCUE is a potential solution for meeting the cryptographic requirements for the NGLD-M which is available as an option for integration by NGLD-M hardware developers. As of FY2022 NGLD-M development will transfer from PE 0303140A, Project DV4 to PE 0605144A, Project BY6 funding line starting FY2022. PE 0605144A, Project BY6 was established to clearly identify requirements for NGLD-M development and is not considered a new start effort.

Project DV5: Crypto Modernization (Crypto Mod) performs test, evaluation, development, and configuration management for cryptographic devices that receive key through fill devices and allow for secure communication through Army devices such as radios and satellite terminals. This program utilizes National Security Agency (NSA) developed Communications Security (COMSEC) technologies within the Army providing encryption, trusted software, or standard operating procedures, and integrating these mechanisms into specified systems in support of securing the Army Tactical and Enterprise Networks. The effort supports network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating networked vulnerabilities to Army information security systems. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army communications systems are required be upgraded to modern algorithms to meet emerging threat developed by our adversaries. Crypto Modernization necessitates the utilization of the latest NSA cryptographic capabilities in order to defeat adversarial efforts to decrypt, disrupt, or exploit US Army networks. COMSEC is the Army's implementation of NSA protections to create a unified network that is protected, resilient, and survivable.

Project DV5 FY 2022 Justification: The program continues testing and evaluation of COMSEC devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Guidance, and new software releases to High Assurance Internet Protocol Encryptor (HAIPE) 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. The program tests interoperability and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Additionally, this program evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	25.710	29.270	28.828	-	28.828
Current President's Budget	25.710	28.270	15.720	-	15.720
Total Adjustments	0.000	-1.000	-13.108	-	-13.108
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-1.000			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-13.108	-	-13.108

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Army	Date: May 2021
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140A *I Information Systems Security Program*

Change Summary Explanation

FY 2022 decrease of $13.108 million based on establishment of the new funding line in support of NGLD-M development. Funding was realigned from PE 0303140A Project DV4 to 0605144A Project BY6 starting in FY 2022.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

COST ($ in Millions)	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	8.368	8.009	6.937	-	6.937	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

PE 0303140A, project 491 includes funding for the Army CIO/G6 and Project Lead (PL) Enterprise Services (ES).

A. Mission Description and Budget Item Justification

Project 491: Information Assurance (IA) Development supports the implementation of National Security Agency (NSA) developed Communications Security (COMSEC) technologies within the Army enterprise and tactical networks by ensuring COMSEC devices/systems are cryptographically interoperable and standard based. This entails architecture studies, technology assessments, secured devices testing, system integration and installation kits development to provide protections for fixed infrastructure post, camps and station networks as well as tactical networks. The cited work is consistent with Army's Mission Command Implementation Plan LOE 1, Network Enable Functions.

IA Development funding Implements, establishes functional and technical boundaries of cryptographic, key management and IA capabilities In Coordination With (ICW) the NSA, the Defense Information Systems Agency (DISA), and Joint Services, to secure National Security Systems (NSS), and National Security Information (NSI). Technical evaluations assess the security, operational effectiveness and network interoperability of advanced concepts/technologies to develop policies, standards, and fundamental building blocks for Army COMSEC capabilities that reduce the risk of future materiel solutions that could underperform and disrupt classified operations.

Develop and publish COMSEC and key management implementation planning guidance to identify, standardize, and govern the insertion of IA capabilities that will bridge operational gaps and support the DoD and NSA mandated requirements to enhance network capacity while providing secure information exchange of voice, video, and data IAW the Army Network Campaign Plan. This will be accomplished by interoperability test and evaluation, standards development, technology roadmap development and System of System Network Vulnerability Assessments (SoS NVA) to provide protections for the Army Integrated Tactical Networks.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Oversight and implementation guidance of emerging Cryptographic and CS capabilities to ensure interoperability to maintain compliance with DoD, NSA, and Army policies and regulations. (CIO/G6)	8.368	8.009	6.937
Description: The program provides oversight and guidance for technical research and evaluation of Cryptographic Modernization (CM) and Key Management (KM) capabilities to ensure IA compliance and interoperability. This effort improves operational effectiveness, ensures efficient implementation, and enhances network performance by deploying standardized COMSEC capabilities that are interoperable and supportable in Army, coalition and Joint operating environments. This program enables the Army to collaborate and participate in Joint and Army capability and technology evaluations efforts to define, improve, develop			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
and publish Cyber Security (CS) standards for new/modernized technology insertion to support the Army future networks and key management enterprise. This effort assesses and defines risk mitigation of CS network vulnerabilities in end-to-end Army network operations and Common Operating Environment. (CIO/G6) ***FY 2021 Plans:*** Will continue to provide oversight for the executions of the Army's COMSEC Modernization initiatives including major ACC updates and replacements of existing devices and systems. Continue to evaluate and test new technologies for Army implementation in support of CM2, KMI migration and S-ICAN/ITN architecture implementation. Continue to provide updated end-to-end, tactical-to-strategic COMSEC standardization and implementation guidance to meet Army?s operational requirements. Continue to assess new key management technologies developed by DoD joint KMI program to determine the maturity for Army fielding to protect and strengthen the Army Network posture. Continue to work with DoD CIO, NSA, DISA and other Services to resolve cryptographic interoperability issues for both embedded and standalone systems and performed risk reduction testing of commercial products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Provide timely test and evaluate results to enable the Army to make sound investment strategic decisions and to reduce or eliminate duplications. Participate in operational assessment of NSA, DoD, Joint Staff and Service led Joint Capability Technology Demonstrations to align new technologies to documented Army and Service capability gaps and requirements for protecting National Security Systems and National Security Information. Continue to update and develop policies to posture Army?s operations to implement innovative cryptographic and key management tools and services. Participated in DoD and Army working groups to develop plans for CM2 implementation. Perform System of System Network Vulnerability Assessments (SoS NVA) to provide protections for the Army Integrated Tactical Networks. ***FY 2022 Plans:*** Will continue to provide oversight for the executions of the Army's COMSEC Modernization initiatives including major ACC updates and replacements of existing devices and systems. Continue to evaluate and test new technologies for Army implementation in support of Cryptographic Modernization 2 (CM2) Transmission Security (TRANSEC) ICD, EKMS Tier 1 to KMI migration, Army last mile advanced key distribution concept development and ITN security architecture implementation. Continue to provide updated end-to-end, tactical-to-strategic COMSEC standardization and implementation guidance to meet Army?s operational requirements. Continue to assess new key management technologies developed by DoD joint KMI program to determine the maturity for Army fielding to protect and strengthen the Army Network posture. Continue to work with DoD CIO, NSA, DISA and other Services to resolve cryptographic interoperability issues for both embedded and standalone systems and performed risk reduction testing of commercial products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Provide timely test and evaluate results to enable the Army to make sound investment strategic decisions and to reduce or eliminate duplications. Participate in operational assessment of NSA, DoD, Joint Staff and Service led Joint Capability Technology Demonstrations to align new technologies to documented Army and			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Service capability gaps and requirements for protecting National Security Systems and National Security Information. Continue to update and develop policies to posture Army?s operations to implement innovative cryptographic and key management tools and services. Participated in DoD and Army working groups to develop plans for CM2 implementation. Perform System of System Network Vulnerability Assessments (SoS NVA) to provide protections for the Army Integrated Tactical Networks. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Funds were reallocated toward other priorities resulting in FY2021 to FY2022 decrease.			
Accomplishments/Planned Programs Subtotals	8.368	8.009	6.937

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• DV5: *Crypto Modernization (Crypto Mod)*	5.655	7.804	7.796	-	7.796	-	-	-	-	-	-
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	66.242	81.156	47.990	-	47.990	-	-	-	-	-	-
• BS9716: *NON PEO-SPARES*	3.857	3.896	3.596	-	3.596	-	-	-	-	-	-

Remarks

D. Acquisition Strategy

The objective of the Cryptographic Systems program is to provide adaptive, flexible, and programmable cryptographic solutions using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic systems. Associated documents include CDD, approved by CIO/G6, 15 Jul 2010; ICD, approved by JROC, 25 Mar 2011; AAO; approved by G3, 15 Dec 2011 and revised and approved, 19 Jun 2015.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PL Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	81.783	-		-		-		-		-	0.000	81.783	-
Big Data Pilot (PL ES-CYBER)	TBD	TBD : FT BELVOIR, VA	9.725	-		-		-		-		-	0.000	9.725	-
Information Assurance System Engineering Support (PL Net E)	C/FFP	DSCI Consulting : APG, MD	7.106	-		-		-		-		-	0.000	7.106	-
Engineering Support (PL Net E)	C/CPFF	CACI : APG, MD	5.018	-		-		-		-		-	0.000	5.018	-
Engineering Support (PL Net E)	C/CPFF	Booz Allen Hamilton : APG, MD	3.408	-		-		-		-		-	0.000	3.408	-
Engineering Support (PL Net E)	C/FP	CSC : APG, MD	16.448	-		-		-		-		-	0.000	16.448	-
		Subtotal	123.488	-		-		-		-		-	0.000	123.488	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support (PL Net E)	C/CPFF	TBD : TBD	1.598	-		-		-		-		-	0.000	1.598	-
Engineering Support (CIO/G-6)	C/FP	CACI : APG, MD	12.363	6.957	Oct 2019	3.400	Oct 2020	5.020	Oct 2020	-		5.020	0.000	27.740	-
System Engineering (CIO/G-6)	SS/LH	AFC C5ISR : APG, MD	9.595	1.002	Oct 2019	2.189	Oct 2020	1.473	Oct 2020	-		1.473	0.000	14.259	-
Engineering Support (CIO/G-6)	C/CPFF	booz Allen Hamiton : APG, MD	10.765	-		1.350	Oct 2020	-		-		-	0.000	12.115	-
Engineering Support (CIO/G-6)	C/FFP	AASKI : Edgewood, MD	6.472	-		0.500		-		-		-	0.000	6.972	-
Service (CIO-G-6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	7.051	0.409	Oct 2019	0.570	Oct 2020	0.444	Oct 2020	-		0.444	0.000	8.474	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	47.844	8.368		8.009		6.937		-		6.937	0.000	71.158	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	171.332	8.368		8.009		6.937		-		6.937	0.000	194.646	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

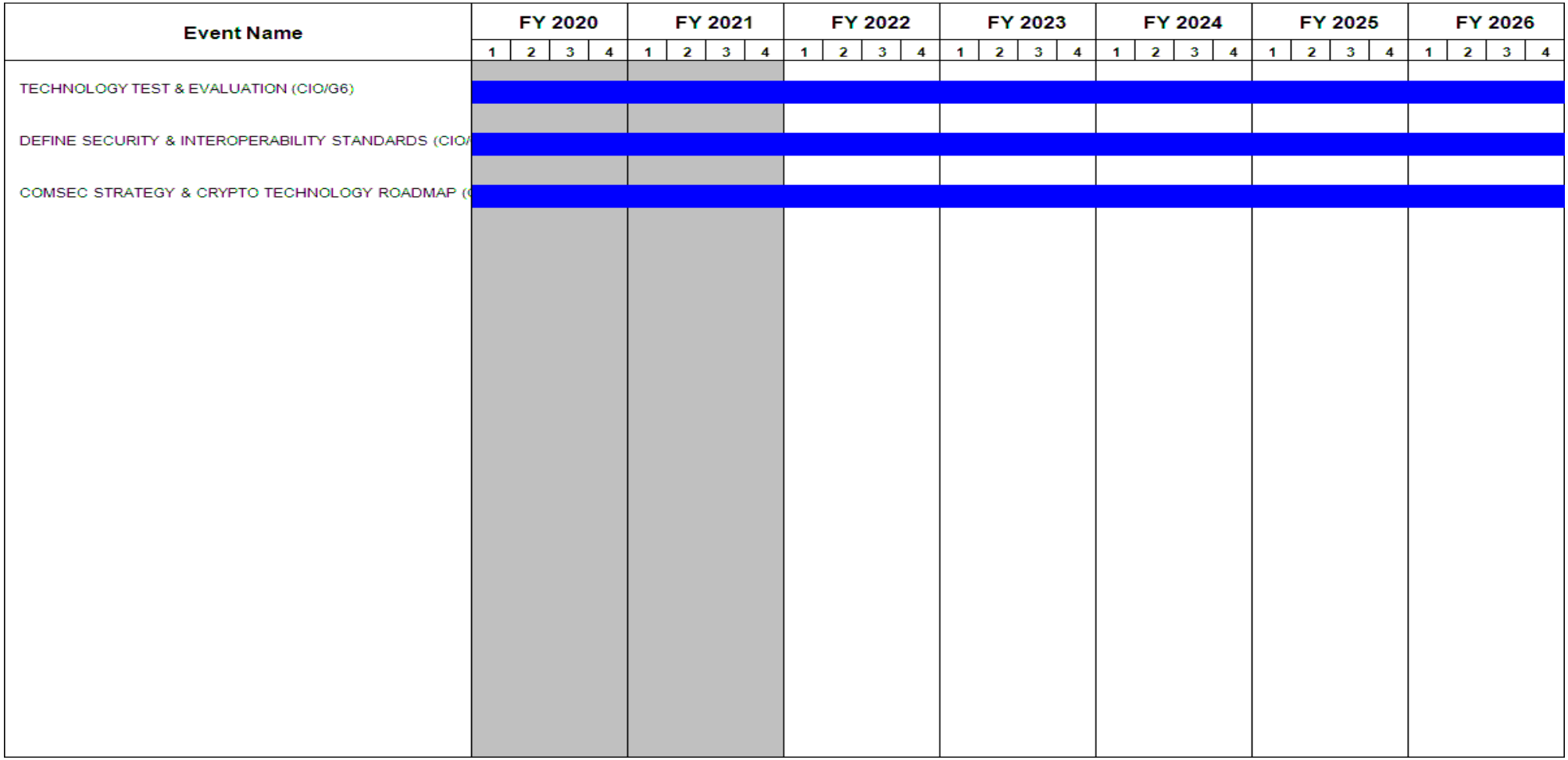

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
TEST & EVALUATION OF CRYPTOGRAPHIC SYSTEMS (PL Net E)	1	2014	4	2014
STUDY OF CURRENT AND EMERGING CRYPTO ALGORITHMS AND TECHNOLOGIES (PL Net E)	1	2015	2	2015
TEST OF INE AND WIRELESS SOLUTION (PL Net E)	1	2016	4	2018
BIG DATA PILOT (PD ES-CYBER)	1	2016	4	2016
TECHNOLOGY TEST & EVALUATION (CIO/G6)	1	2017	4	2027
DEFINE SECURITY & INTEROPERABILITY STANDARDS (CIO/G6)	1	2017	4	2027
COMSEC STRATEGY & CRYPTO TECHNOLOGY ROADMAP (CIO/G6)	1	2014	4	2027

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army											Date: May 2021	
Appropriation/Budget Activity 2040 / 7					R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*				Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*			
COST ($ in Millions)	**Prior Years**	**FY 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
DV4: *Key Management Infrastructure (KMI)*	-	11.687	12.457	0.987	-	0.987	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This funding line supports the Army Network Modernization Strategy LOE 1, Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy.

Communications Security (COMSEC) is governed by the Chairman of the Joint Chiefs of Staff Instruction (CJCSA) 6510. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army communications systems are required to support modern cryptographic capabilities by implementing modern algorithms.

As part of the Army's Key Management Infrastructure (KMI) implementation, the Next Generation Load Device - Medium (NGLD-M) is an Acquisition Category III (ACAT III) Program of Record (POR). The NGLD-M requires RDT&E investment to develop and test the hardware and software solutions to meet the operational requirements outlined in the NGLD Capability Production Document (CPD) to modernize fill devices with capability to transfer and receive cryptographic key over a network to reduce causalities and maintain mission OPTEMPO. Without this technology Warfighters are required to manually receive their cryptographic products by traveling to COMSEC account locations (which may not be co-located) and manually filling their devices.

The Reprogrammable Single Chip Universal Encryptor (RESCUE) is a government owned reprogrammable cryptographic chip that incorporates KMI functionality and modern algorithms to encrypt and decrypt messages for the embedding. This chip could be adapted for use within the NGLD-M or any other cryptographic communications system.

NGLD-M development will be realigned to 0605144A/BY6 funding line starting FY2022.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Reprogrammable Cryptographic Chip Development and Evaluation	1.000	1.000	0.987
Description: The Reprogrammable Single Chip Universal Encryptor (RESCUE) is a reprogrammable cryptographic chip that incorporates KMI functionality and modern algorithms to encrypt and decrypt messages for the embedding device. The RESCUE is built upon a modular architecture to enable tailoring of the chip to meet the specific requirements of the embedding device. This effort creates a government owned potential universal cryptographic chip enabling the Army to decrease costs for encryption devices.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
FY 2021 Plans: The RESCUE effort will consist of maintaining lab equipment, embedment planning to utilize the RESCUE chip with new capabilities, requirements analysis, tracking part's obsolescence, and software/firmware baseline development. ***FY 2022 Plans:*** The RESCUE effort will consist of maintaining lab equipment, embedment planning to utilize the RESCUE chip with new capabilities, requirements analysis, tracking part's obsolescence, and software/firmware baseline development. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Mission requirements changed.			
Title: NGLD Medium Development and NSA Certification ***Description:*** The Next Generation Load Device - Medium (NGLD-M) will conduct the Army's key fill mission by issuing, filling, and managing Cryptographic keys to both legacy and future KMI aware End-Cryptographic Units (ECUs). This technology requires RDT&E investment to meet the requirements outlined in the NGLD Capability Production Document (CPD). NGLD-M development will be realigned to 0605144A/BY6 funding line starting FY2022. ***FY 2021 Plans:*** Support NGLD-M system integration and the User Application Software (UAS) which is a graphical interface that will allow users to interact with the device. The NGLD-M development will establish configuration items and allocate system functions and performance requirements to the configurations items through a Preliminary Design Review. Further NGLD-M development will finalize the physical and functional characteristics of the NGLD-M configuration items and establish Government configuration control of the design at the Critical Design Review (CDR). At CDR, The Government will receive pre-production development models to support Highly Accelerated Life Testing for system reliability testing, End Cryptographic Unit interoperability testing, and the Risk Management Framework Security Control Assessment. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** This effort will be funded by a new NGLD-M BA 5 funding line.	10.578	11.346	-
Title: Program Management Support ***Description:*** PMO costs will be covered by OMA funding. This funds a matrixed Acquisition Program Manager (APM) from Combat Capabilities Development Command (CCDC) Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to manage the NGLD-M development effort. ***FY 2021 Plans:***	0.109	0.111	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
FY 2021 funds a matrixed Acquisition Program Manager (APM) from Combat Capabilities Development Command (CCDC) Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to manage the NGLD-M development effort. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** This effort will be funded by a new NGLD-M BA 5 funding line.			
Accomplishments/Planned Programs Subtotals	11.687	12.457	0.987

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• B96004: *KEY MANAGEMENT INFRASTRUCTURE*	80.855	78.244	78.283	-	78.283	-	-	-	-	-	-
• OMA - 153140: *ISSP (TSEC-AKMS)*	-	-	-	-	-	-	-	-	-		

Remarks

Line Item & Title:
B96004: Key Management Infrastructure (OPA2)
153140: ISSP (TSEC-AKMS) (OMA)

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) acquisition strategy consists of Army, Air Force, and NSA Programs of Record (POR). AKMI is the Army's implementation of the National Security Agency (NSA) Key Management Infrastructure (KMI) ACAT IAM Program of Record. The AKMI will allow the Army to manage, control, plan, and distribute electronic key for the ~1.5 million End Cryptographic Units (ECU)s necessary to communicate and distribute data on the Army's tactical and strategic networks such as radios, secure phones, and satellite terminals.

The AKMI Program includes the Simple Key Loader (SKL) and Automated Communications Engineering Software (ACES) workstation contracts managed by the Army, Tactical Key Loader (TKL) contract by the US Air Force, and the Management Clients (MGC) nodes by NSA.

The AKMI program funded development of a KMI compliant cryptographic engine, the government owned
Reprogrammable Single Chip Universal Encryptor (RESCUE) that can be utilized by NGLD-M or other COMSEC devices. The NGLD-M will undergo full-and-open competition for development, production, and sustainment with a projected FY21 award.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

The Milestone Decision Authority issued a Materiel Development Decision (MDD) Acquisition Decision Memorandum (ADM) on 14 March 2019 that designated the NGLD-M as an ACAT III Program of Record (PoR) and authorized execution of FY2019-FY2021 RDT&E funds for acquisition planning and risk mitigation.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
FY 2018 NDAA SEC 825 MDAP Cost Overrun	SS/CR	APG, MD : APG, MD	0.044	-		-		-		-		-	0.000	0.044	-
		Subtotal	0.044	-		-		-		-		-	0.000	0.044	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
KMI Awareness (RESCUE Development and NSA Certification	C/CPFF	Dynamics Research Corporation/Engility : APG, MD	14.445	1.000	Jul 2020	1.000	Jul 2021	0.987	Jul 2022	-		0.987	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CCDC C5ISR, S&TCD : APG, MD	1.451	-		-		-		-		-	0.000	1.451	-
NGLD Development	C/CPFF	CCDC C5ISR S&TCD; NAVWARSYSCOM : APG, MD; San Diego, CA; TBD	1.250	10.578	Nov 2019	11.346	Nov 2020	-		-		-	Continuing	Continuing	Continuing
		Subtotal	17.146	11.578		12.346		0.987		-		0.987	Continuing	Continuing	N/A

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Support	C/CPFF	CCDC C5ISR S&TCD : APG, MD	-	0.109	Nov 2019	0.111	Nov 2020	-		-		-	0.000	0.220	-
		Subtotal	-	0.109		0.111		-		-		-	0.000	0.220	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	17.190	11.687		12.457		0.987		-		0.987	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*	

	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

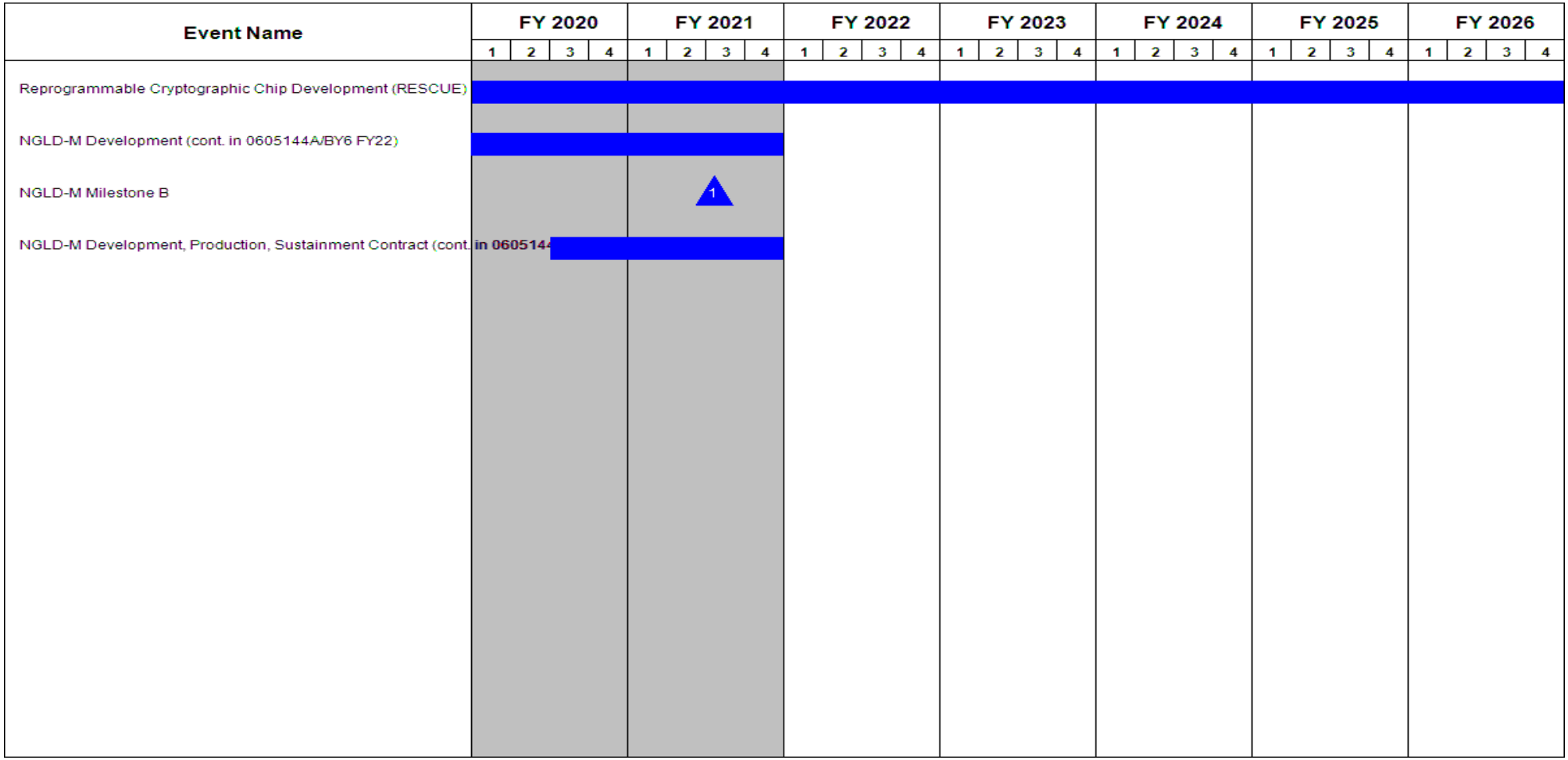

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Reprogrammable Cryptographic Chip Development (RESCUE)	1	2019	4	2026
NGLD-M Development (cont. in 0605144A/BY6 FY22)	2	2019	4	2021
NGLD-M Milestone B	3	2021	3	2021
NGLD-M Development, Production, Sustainment Contract (cont. in 0605144A/BY6 FY22	3	2020	4	2021
NGLD-M Simplified Acquisition Management Plan	4	2019	4	2019

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

COST ($ in Millions)	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	5.655	7.804	7.796	-	7.796	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Project DV5, Crypto Modernization (Crypto Mod), supports the Army Network Modernization Strategy LOE 1, Unified Network. Efforts are aligned to support the Network-Cross Functional Team capability set approach to achieve the network modernization strategy. Communications Security (COMSEC) is governed by the Chairman of the Joint Chiefs of Staff Instruction (CJCSA) 6510.

Crypto Mod performs test, evaluation, development, and configuration management for cryptographic devices that receive key through fill devices and allow for secure communication through Army devices such as radios and satellite terminals. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army communications systems are required be upgraded to modern algorithms to meet emerging threat developed by our adversaries. Crypto Modernization necessitates the utilization of the latest National Security Agency (NSA) cryptographic capabilities in order to defeat adversarial efforts to decrypt, disrupt, or exploit US Army networks. Communications Security (COMSEC) is the Army's implementation of NSA protections to create a unified network that is protected, resilient, and survivable.

To accomplish this multi-faceted effort, consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan, Crypto Mod performs evaluation of emerging threats, development of advances protections to defeat these threats, testing of commercial and government off the shelf applications developed to provide protections against identified threats, and assessment of new software and hardware updates to these end user devices and software to ensure they remain hardened against cyber-attack. This ensures that all endpoints from singular NIPRNET, SIPRNET, JWICS and Intelligence workstations in the strategic Enterprise to Tactical vehicles and equipment utilized by dismounted personnel forward deployed in hot zone are protected when processing the critical mission and voice data that provides the strategic overmatch required to accomplish the Army's mission.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.746	0.300	0.306
Description: This program researches, assesses, tests, plans and works to integrate VACM products for the Army. These are a critical voice communications asset utilized for the president's air wing. The VACM program is a NSA mandated program established to replace legacy external cryptographic devices such as the KY-57, KY-99A, KY-58, KY-99, KY-100 and CV- 3591 / KYV-5. In order to ensure the confidentiality, integrity and availability of classified communications, the cryptographic modules must be tested for interoperability and form fit to ensure a successful fielding. Each software release will require testing to insure comparability and interoperability.			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
FY 2021 Plans: The program will continue to test and evaluate new software update to VACM devices to confirm continued capability and interoperability on Army networks and different tactical platforms as well as identifying new risk areas for compliance with COMSEC regulations and procedures. Development activities are ongoing as programs continue fielding, performing site surveys and installing at both CONUS and OCONUS locations. ***FY 2022 Plans:*** The program will continue to test and evaluate new software update to VACM devices to confirm continued capability and interoperability on Army networks and different tactical platforms as well as identifying new risk areas for compliance with COMSEC regulations and procedures. Development activities are ongoing as programs continue fielding, performing site surveys and installing at both CONUS and OCONUS locations. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The increase is due to the inflation.			
Title: Cryptographic Systems Test and Evaluation ***Description:*** This program supports the Army Cryptographic Modernization Transformational Initiative. This is accomplished by providing test and evaluation capabilities to the COMSEC community in order to assess emerging technologies before being released and approved for Army use; testing will be performed on hardware, software and network systems. ***FY 2021 Plans:*** Conduct testing and evaluation of COMSEC devices Link Encryptor Family (LEF), In-Line Network Encryptor (INE), Secure Voice (SV) to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures, with particular emphasis on the Advanced Cryptographic Capabilities (ACC) program lead by the NSA. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Guidance and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. These devices provides the critical security backbone for all NIPRNET, SIPRNET, JWICS and Intelligence networks in both the Tactical and Enterprise networks. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure to defend against adversary attack and exploitation. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure. Additionally, this program evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2022 Plans:***	3.944	6.520	6.486

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Conduct testing and evaluation of COMSEC devices Link Encryptor Family (LEF), In-Line Network Encryptor (INE), Secure Voice (SV) to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures, with particular emphasis on the Advanced Cryptographic Capabilities (ACC) program lead by the NSA. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Guidance and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. These devices provides the critical security backbone for all NIPRNET, SIPRNET, JWICS and Intelligence networks in both the Tactical and Enterprise networks. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure to defend against adversary attack and exploitation. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure. Additionally, this program evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** Change in mission requirements.			
Title: High Assurance Internet Protocol Encryption (HAIPE) extension manager ***Description:*** A management tool to configure the new extensions to the HAIPE standard and process the resulting data to provide early indications of cyber attacks. ***FY 2021 Plans:*** The program will continue software development efforts that will provide configuration and management of the HAIPE extensions and the user interface for collecting and analyzing the data that results from implementation of these HAIPE extensions. Addition of ACC software feature and new devices will be implemented. This will also facilitate the upgrade of the Army HAIPE to include new cyber sensor functionality for the tactical cell. ***FY 2022 Plans:*** The program will continue software development efforts that will provide configuration and management of the HAIPE extensions and the user interface for collecting and analyzing the data that results from implementation of these HAIPE extensions. Addition of ACC software feature and new devices will be implemented. This will also facilitate the upgrade of the Army HAIPE to include new cyber sensor functionality for the tactical cell. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** The increase is due to the inflation.	0.965	0.984	1.004
Accomplishments/Planned Programs Subtotals	5.655	7.804	7.796

Exhibit R-2A, RDT&E Project Justification: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	66.242	81.156	47.990	-	47.990	-	-	-	-	-	-
• BS9716: *NON PEO-SPARES*	3.857	3.896	3.596	-	3.596	-	-	-	-	-	-

Remarks

Line Item & Title:
B96002 - Cryptographic Systems - OPA2
BS9716 - NON PEO-SPARES - OPA4

D. Acquisition Strategy

The Cryptographic Systems procures NSA IDIQ contracts. Army RDT&E is used on existing and emerging encryptors which are tested and evaluated for Functionality, Security, Interoperability, and backward compatibility on software and hardware for both Tactical and Enterprise systems to ensure they remain hardened against cyberattack. CDD, approved by CIO/G6, 15 Jul 2010; ICD, approved by JROC, 25 Mar 2011; AAO; approved by G3, 15 Dec 2011 and revised and approved, 19 Jun 2015.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CCDC C5ISR S&TCD : APG, MD	6.093	0.525	Nov 2019	0.540	Nov 2020	0.545	Nov 2021	-		0.545	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	7.442	0.340	Feb 2020	0.310	Feb 2021	0.315	Feb 2022	-		0.315	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	4.332	0.578	Feb 2020	0.234	Feb 2021	0.235	Feb 2022	-		0.235	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	5.566	0.268	Apr 2020	0.200	Apr 2021	0.205	Apr 2022	-		0.205	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/CPFF	Envision : Aberdeen, Maryland	0.966	-		-		-		-		-	0.000	0.966	Continuing
Embedded Crypto Modernization Support	C/LH	Canceled : Canceled	37.770	-		-		-		-		-	0.000	37.770	-
		Subtotal	62.169	1.711		1.284		1.300		-		1.300	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test & Evaluation	SS/LH	CCDC C5ISR S&TCD : APG, MD	0.262	0.272	Nov 2019	1.300	Nov 2020	1.301	Nov 2021	-		1.301	0.000	3.135	-
Test & Evaluation	C/CPFF	CACI : APG, MD	2.485	1.756	Feb 2020	1.800	Feb 2021	1.792	Feb 2022	-		1.792	0.000	7.833	-
Test & Evaluation	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.985	1.057	Feb 2020	1.820	Feb 2021	1.812	Feb 2022	-		1.812	0.000	5.674	-
Test & Evaluation	C/CPFF	AASKI : APG, MD	0.640	0.859	Apr 2020	1.600	Apr 2021	1.591	Apr 2022	-		1.591	0.000	4.690	-
		Subtotal	4.372	3.944		6.520		6.496		-		6.496	0.000	21.332	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	66.541	5.655		7.804		7.796		-		7.796	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Army			Date: May 2021
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

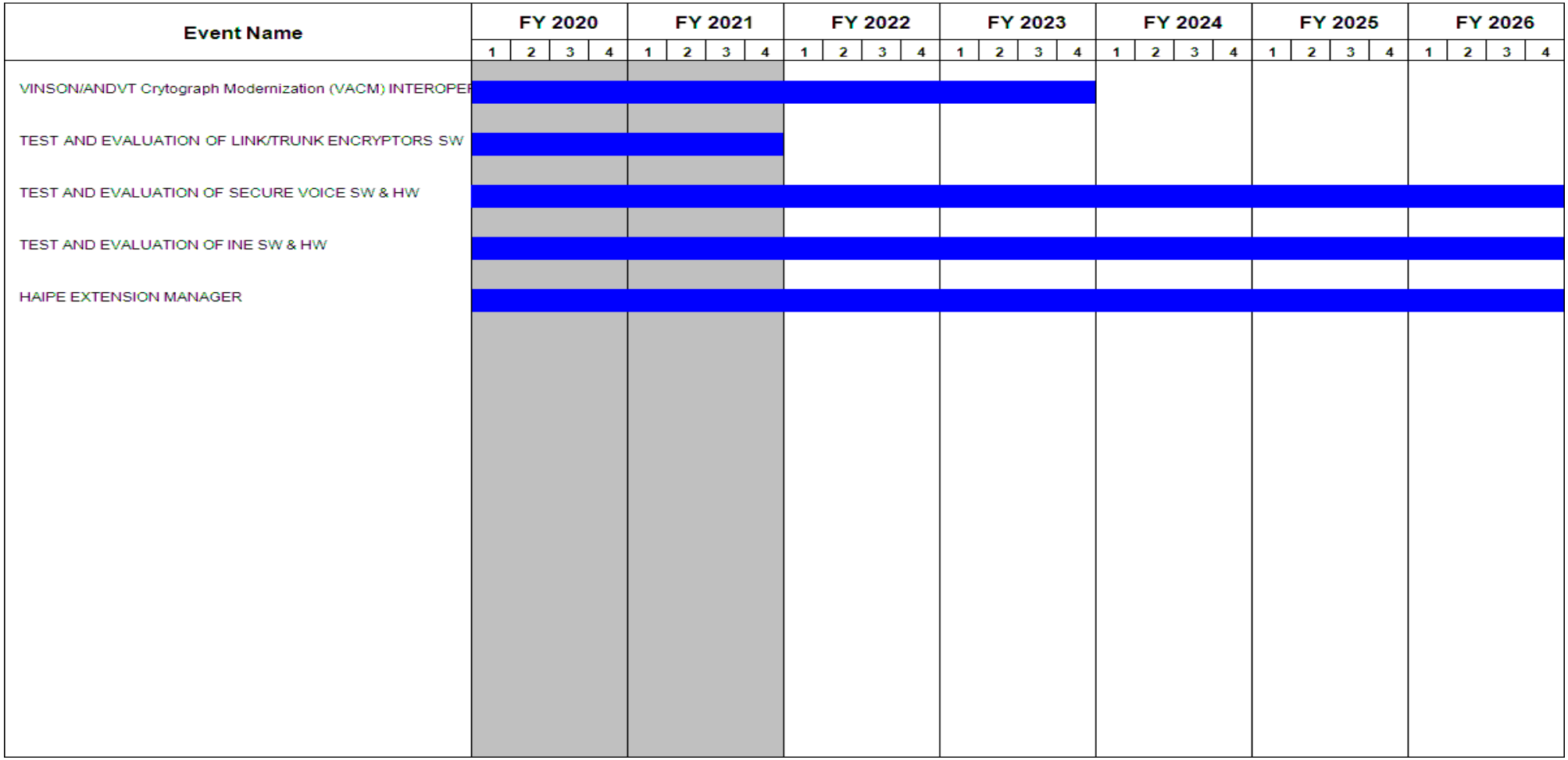

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Army		Date: May 2021
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
VINSON/ANDVT Crytograph Modernization (VACM) INTEROPERABILITY	1	2016	4	2023
TEST AND EVALUATION OF LINK/TRUNK ENCRYPTORS SW	1	2016	4	2021
TEST AND EVALUATION OF SECURE VOICE SW & HW	4	2013	4	2026
TEST AND EVALUATION OF INE SW & HW	1	2017	4	2026
HAIPE EXTENSION MANAGER	1	2017	4	2026