Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army											Date: April 2022	
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 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**Cost To Complete**	**Total Cost**
Total Program Element	-	28.270	15.680	17.209	-	17.209	16.675	18.140	18.146	18.323	Continuing	Continuing
491: *Information Assurance Development*	-	8.009	6.937	7.816	-	7.816	7.184	8.202	8.205	8.285	Continuing	Continuing
DV4: *Key Management Infrastructure (KMI)*	-	12.457	0.987	1.023	-	1.023	1.027	1.435	1.436	1.450	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	7.804	7.756	8.370	-	8.370	8.464	8.503	8.505	8.588	Continuing	Continuing

A. Mission Description and Budget Item Justification

A portion of this funding line is a key enabler of the Army Modernization Priorities in support of the Communications Security (COMSEC) Key Management Infrastructure (KMI) program.

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 2023 Army	Date: April 2022
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 tactical networks/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.

Project 491 FY 2023 Justification: The program 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 tactical network/architecture future Capability Set developments. Provide proof of concepts 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.

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 are key enablers of the Army Modernization Priorities in support of LOE 1, Unified Network.

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 2023 Justification: This funding line supports COMSEC technologies within the Army, specifically, 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. 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 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 to 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 2023 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 770-03 dated 16 July 2021. 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Army					Date: April 2022
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*		
B. Program Change Summary ($ in Millions)	**FY 2021**	**FY 2022**	**FY 2023 Base**	**FY 2023 OCO**	**FY 2023 Total**
Previous President's Budget	28.270	15.720	0.000	-	0.000
Current President's Budget	28.270	15.680	17.209	-	17.209
Total Adjustments	0.000	-0.040	17.209	-	17.209
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	17.209	-	17.209
• FFRDC Transfer	-	-0.040	-	-	-

Change Summary Explanation

Fiscal Year 2023 (FY23) funding increase reflects the fact that the FY22 President's Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	8.009	6.937	7.816	-	7.816	7.184	8.202	8.205	8.285	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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 2021	FY 2022	FY 2023
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)	8.009	6.937	7.816
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 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)			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
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 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 2023 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 Service capability gaps and requirements for protecting National Security Systems and National Security Information. Continue to			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
update and develop policies to posture Army?s operations to implement innovative cryptographic and key management tools and services. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** Increase to assess new security standards benchmarks to align with the DoD ACC mandates and to report Army's compliance and frequency of modernization initiative to reduce risk and duplications			
Accomplishments/Planned Programs Subtotals	8.009	6.937	7.816

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
• DV5: *Crypto Modernization (Crypto Mod)*	7.804	7.756	8.370	-	8.370	8.464	8.503	8.505	8.588	Continuing	Continuing
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	81.156	47.990	50.151	-	50.151	51.403	56.832	57.000	56.975	0.000	401.507
• BS9716: *NON PEO-SPARES*	3.896	3.596	4.014	-	4.014	3.743	4.063	4.073	4.072	0.000	27.457

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 2023 Army		Date: April 2022
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 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 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 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 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	19.320	3.400	Oct 2020	5.020	Oct 2021	3.600	Oct 2022	-		3.600	0.000	31.340	-
System Engineering (CIO/G-6)	SS/LH	AFC C5ISR : APG, MD	10.597	2.189	Oct 2020	1.473	Oct 2021	2.345	Oct 2022	-		2.345	0.000	16.604	-
Engineering Support (CIO/G-6)	C/CPFF	booz Allen Hamiton : APG, MD	10.765	1.350	Oct 2020	-		1.480	Oct 2022	-		1.480	0.000	13.595	-
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)	7.460	0.570	Oct 2020	0.444	Oct 2021	0.391	Oct 2022	-		0.391	0.000	8.865	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2023 Army			Date: April 2022
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 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	56.212	8.009		6.937		7.816		-		7.816	0.000	78.974	N/A

	Prior Years	FY 2021		FY 2022		FY 2023 Base		FY 2023 OCO		FY 2023 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	179.700	8.009		6.937		7.816		-		7.816	0.000	202.462	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2023 Army		Date: April 2022
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

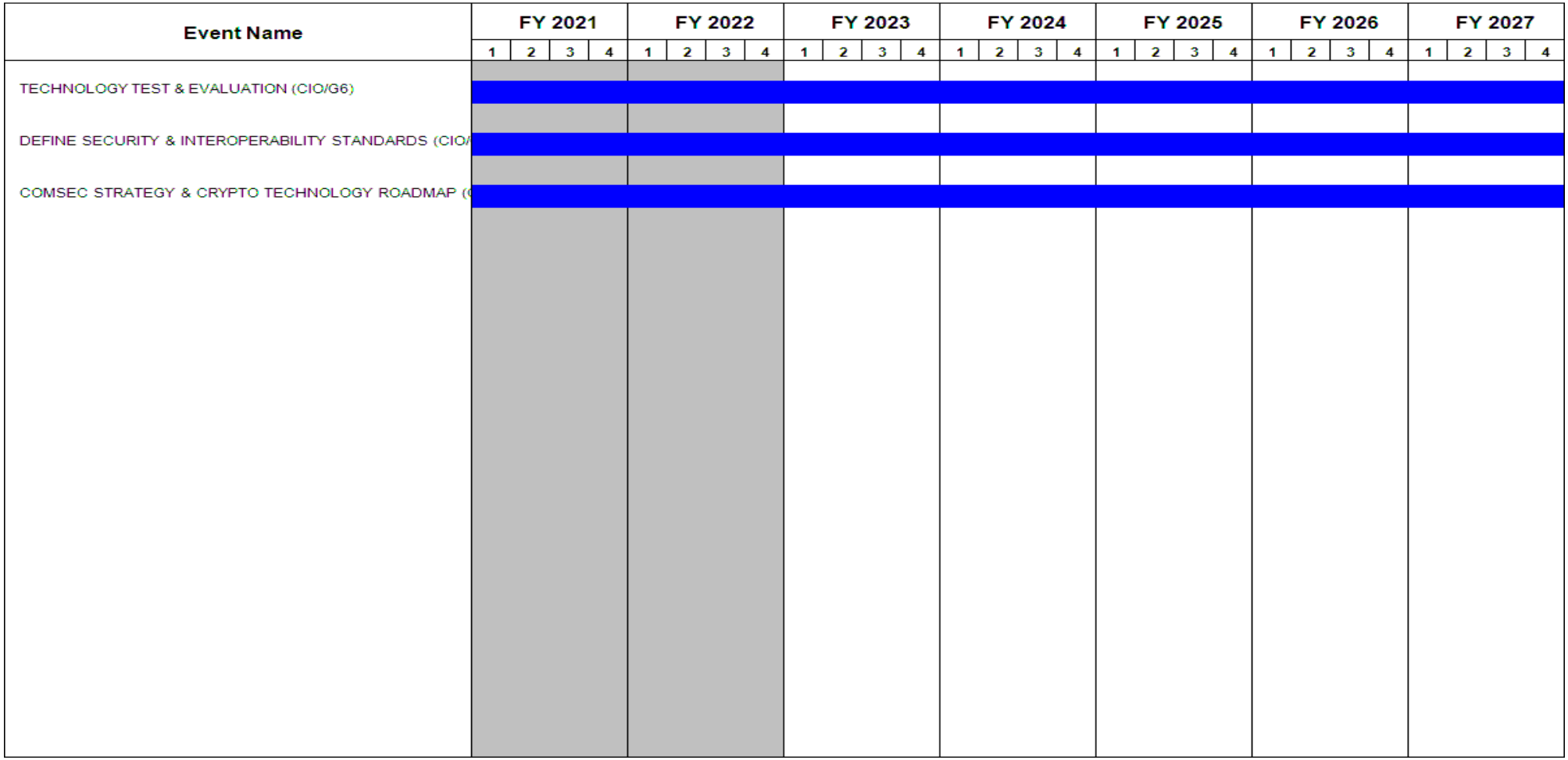

Exhibit R-4A, RDT&E Schedule Details: PB 2023 Army		Date: April 2022
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

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 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
DV4: *Key Management Infrastructure (KMI)*	-	12.457	0.987	1.023	-	1.023	1.027	1.435	1.436	1.450	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This funding line is a key enabler of the Army Modernization Priorities in support of LOE 1, Unified Network.

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.

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

FY 2023 funds will support COMSEC technologies within the Army, specifically, 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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Reprogrammable Cryptographic Chip Development and Evaluation	1.087	0.987	1.023
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.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
This effort creates a government owned potential universal cryptographic chip enabling the Army to decrease costs for encryption devices. ***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 2023 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 to FY 2023 Increase/Decrease Statement:*** The increase is due to inflation.			
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 was realigned to 0605144A/BY6 funding line starting FY2022.	11.259	-	-
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.	0.111	-	-
Accomplishments/Planned Programs Subtotals	12.457	0.987	1.023

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
• B96004: *KEY MANAGEMENT INFRASTRUCTURE*	78.244	78.283	75.541	-	75.541	87.744	93.561	93.835	93.794	0.000	601.002
• OMA - 153140: *ISSP (TSEC-AKMS)*	-	-	-	-	-	-	-	-	-		

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost

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 underwent full-and-open competition for development, production, and sustainment and awarded contracts on 10 August 2021. 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 2023 Army			Date: April 2022
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 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 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 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 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	15.445	1.087	Jul 2021	0.987	Jul 2022	1.023	Jul 2022	-		1.023	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; GDMS; SNC : APG, MD; San Diego, CA; Dedham, MA; Sparks, NV	11.828	11.259	Nov 2020	-		-		-		-	Continuing	Continuing	Continuing
		Subtotal	28.724	12.346		0.987		1.023		-		1.023	Continuing	Continuing	N/A

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Support	C/CPFF	CCDC C5ISR S&TCD : APG, MD	0.109	0.111	Nov 2020	-		-		-		-	0.000	0.220	-
		Subtotal	0.109	0.111		-		-		-		-	0.000	0.220	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2023 Army			Date: April 2022
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 2021		FY 2022		FY 2023 Base		FY 2023 OCO		FY 2023 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	28.877	12.457		0.987		1.023		-		1.023	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2023 Army		Date: April 2022
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)*

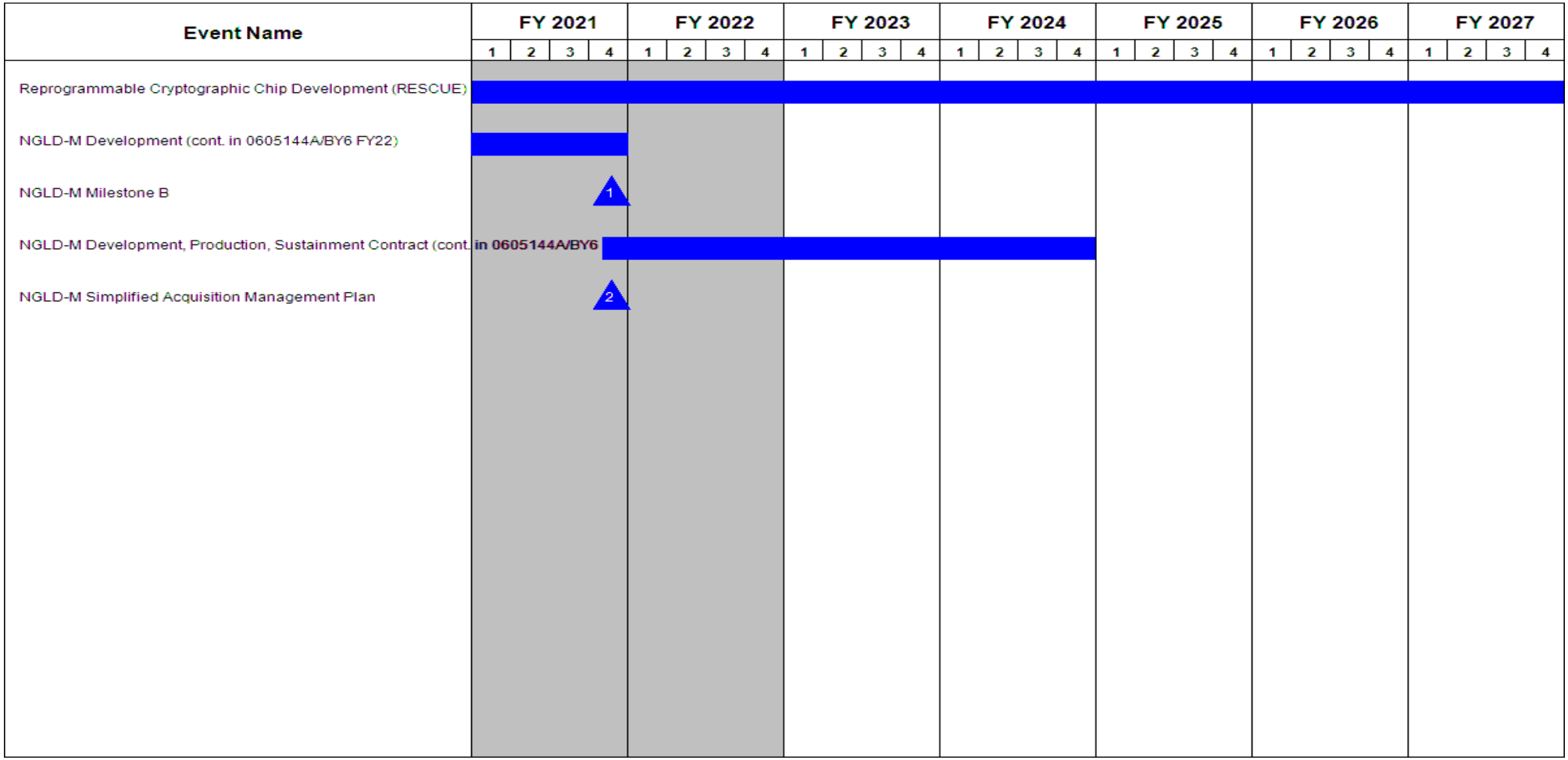

Exhibit R-4A, RDT&E Schedule Details: PB 2023 Army		Date: April 2022
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Reprogrammable Cryptographic Chip Development (RESCUE)	1	2019	4	2027
NGLD-M Development (cont. in 0605144A/BY6 FY22)	2	2019	4	2021
NGLD-M Milestone B	4	2021	4	2021
NGLD-M Development, Production, Sustainment Contract (cont. in 0605144A/BY6 FY22	4	2021	4	2024
NGLD-M Simplified Acquisition Management Plan	4	2021	4	2021

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	7.804	7.756	8.370	-	8.370	8.464	8.503	8.505	8.588	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This funding line is a key enabler of the Army Modernization Priorities in support of LOE 1, Unified Network.

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 to 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.

FY 2023 funds will support the testing of all existing and emerging encryptors for Functionality, Security, and Interoperability.The program will continue 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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.300	0.306	0.329

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
Description: This program researches, assesses, tests, plans and works to integrate VACM products for the Army. 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. ***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 2023 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 to FY 2023 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 2022 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)	5.876	5.789	6.258

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
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 2023 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. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The increase is due to the inflation.			
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 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 2023 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. ***FY 2022 to FY 2023 Increase/Decrease Statement:***	0.984	1.004	1.078

Exhibit R-2A, RDT&E Project Justification: PB 2023 Army		Date: April 2022
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 2021	FY 2022	FY 2023
The increase is due to the inflation.			
Title: Program Management Office Support	0.644	0.657	0.705
Description: Program management includes overall management of program execution, major events, reporting, funds execution, contract management, and logistical support. Includes participation in program planning and Integrated Product Team meetings. ***FY 2022 Plans:*** FY22 funds will provide overall management and oversight to implement Crypto Mod test, evaluation, development and configuration management for cryptographic devices - to include Matrix and Contractor support. ***FY 2023 Plans:*** FY 2023 funds will provide overall management and oversight to implement Crypto Mod test, evaluation, development and configuration management for cryptographic devices - to include Matrix and Contractor support. ***FY 2022 to FY 2023 Increase/Decrease Statement:*** The increase is due to inflation			
Accomplishments/Planned Programs Subtotals	7.804	7.756	8.370

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	81.156	47.990	50.151	-	50.151	51.403	56.832	57.000	56.975	0.000	401.507
• BS9716: *NON PEO-SPARES*	3.896	3.596	4.014	-	4.014	3.743	4.063	4.073	4.072	0.000	27.457

Remarks

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

D. Acquisition Strategy

The Cryptographic Systems procures off of 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 2023 Army			Date: April 2022
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)*	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Office Support	Various	PEO C3T & CECOM : Various; APG, MD	-	0.644	Dec 2020	0.657	Dec 2021	0.705	Dec 2022	-		0.705	0.000	2.006	-
		Subtotal	-	0.644		0.657		0.705		-		0.705	0.000	2.006	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CCDC C5ISR S&TCD : APG, MD	6.618	1.011	Nov 2020	1.031	Nov 2021	1.107	Nov 2022	-		1.107	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	7.782	0.637	Feb 2021	0.650	Feb 2022	0.698	Feb 2023	-		0.698	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	4.910	0.267	Feb 2021	0.272	Feb 2022	0.292	Feb 2023	-		0.292	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	5.834	-		-		-		-		-	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	63.880	1.915		1.953		2.097		-		2.097	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test & Evaluation	SS/LH	CCDC C5ISR S&TCD : APG, MD	0.534	1.637	Nov 2020	1.670	Nov 2021	1.793	Nov 2022	-		1.793	0.000	5.634	-
Test & Evaluation	C/CPFF	CACI : APG, MD	4.241	3.608	Feb 2021	3.476	Feb 2022	3.775	Feb 2023	-		3.775	0.000	15.100	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2023 Army			Date: April 2022
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)*	

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2021 Cost	FY 2021 Award Date	FY 2022 Cost	FY 2022 Award Date	FY 2023 Base Cost	FY 2023 Base Award Date	FY 2023 OCO Cost	FY 2023 OCO Award Date	FY 2023 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test & Evaluation	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	2.042	-		-		-		-		-	0.000	2.042	-
Test & Evaluation	C/CPFF	AASKI : APG, MD	1.499	-		-		-		-		-	0.000	1.499	-
		Subtotal	8.316	5.245		5.146		5.568		-		5.568	0.000	24.275	N/A

	Prior Years	FY 2021		FY 2022		FY 2023 Base		FY 2023 OCO		FY 2023 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	72.196	7.804		7.756		8.370		-		8.370	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2023 Army		Date: April 2022
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)*

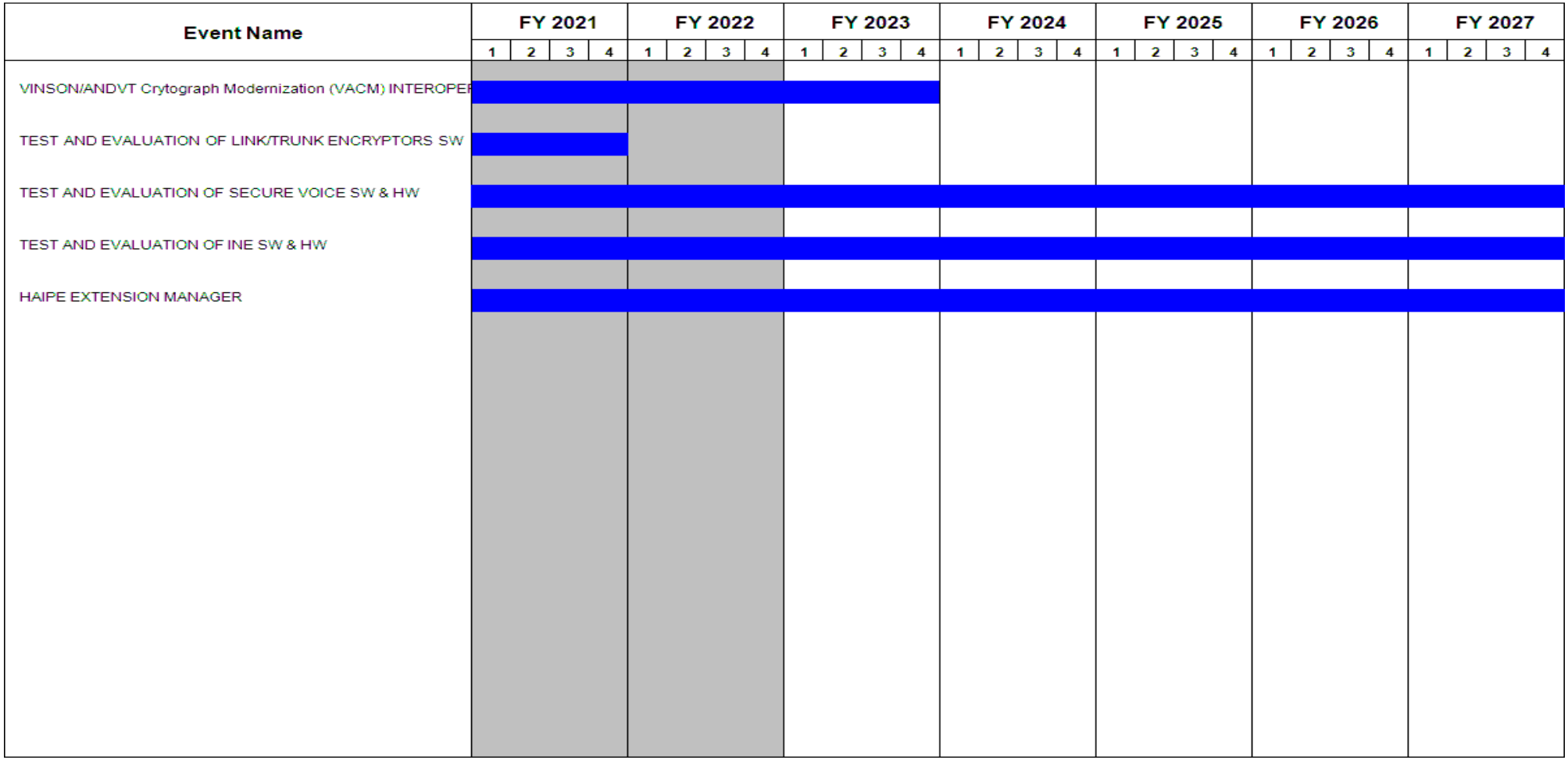

Exhibit R-4A, RDT&E Schedule Details: PB 2023 Army		Date: April 2022
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

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	2035
TEST AND EVALUATION OF INE SW & HW	1	2017	4	2035
HAIPE EXTENSION MANAGER	1	2017	4	2035