Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army											Date: March 2023	
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**Cost To Complete**	**Total Cost**
Total Program Element	-	15.680	17.209	15.323	-	15.323	17.786	17.807	17.998	18.200	Continuing	Continuing
491: *Information Assurance Development*	-	6.937	7.816	7.035	-	7.035	8.042	8.052	8.138	8.229	Continuing	Continuing
DV4: *Key Management Infrastructure (KMI)*	-	0.987	1.023	-	-	-	1.407	1.409	1.425	1.441	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	7.756	8.370	8.288	-	8.288	8.337	8.346	8.435	8.530	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 Chief Information Officer/Deputy Chief of Staff, G-6 manages Information Assurance Development.

Project 491: 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 includes 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 2024 Army	Date: March 2023
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*

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: Key Management Infrastructure (KMI) & DV5: Crypto Modernization (Crypto Mod). 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: KMI. 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 DV5: Crypto Modernization (Crypto Mod). 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

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Army	Date: March 2023
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*

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 DV4: KMI has no funding request in FY 2024.

Crypto Mod continues testing and evaluation of COMSEC devices in FY 2024 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.

B. Program Change Summary ($ in Millions)	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total
Previous President's Budget	15.680	17.209	16.675	-	16.675
Current President's Budget	15.680	17.209	15.323	-	15.323
Total Adjustments	0.000	0.000	-1.352	-	-1.352
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-1.352	-	-1.352

Change Summary Explanation

FY 2024 funding decrease of $1.352 million. $1.001 million of this decrease is based on the realignment from PE 0303140A Information Systems Security Project, Project DV4: Key Management Infrastructure to PE 0605144A, Next Generation Load Device - Medium, Project BY6: Key Management Infrastructure Development. Decrease of $0.418 million due to higher Army priorities. Increase of $.067 million due to economic assumptions.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	6.937	7.816	7.035	-	7.035	8.042	8.052	8.138	8.229	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 2022	FY 2023	FY 2024
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/G-6)	6.937	7.816	7.035
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/G-6)			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 update and develop policies to posture Army's operations to implement innovative cryptographic and key management tools and services.			
FY 2024 Plans: Continue to provide oversight for the executions of the Army's Communications Security (COMSEC) Modernization initiatives including major Advanced Cryptographic Capabilities (ACC) and Cryptographic Modernization 2 (CM2) updates and replacements of existing devices and systems. Continue to evaluate and test emerging technologies for Army implementation in support of, Transmission Security (TRANSEC) Initial Capabilities Document (ICD), Electronic Key Management System (EKMS) Tier 1 to Key Management Infrastructure (KMI) migration, Army last mile advanced key distribution concept development and Multi-Domain Operations (MDO) 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 NSA's KMI program to determine the maturity for Army fielding to protect and strengthen the Army Unified Network posture. Continue to work with DoD CIO, Joint Staff, NSA, DISA and other Services to resolve cryptographic interoperability issues for both embedded and standalone cryptographic devices/systems and perform risk reduction testing of commercial cryptographic products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Provide timely test and evaluation results to enable the Army to make sound strategic investment 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 DoD capability gaps			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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. ***FY 2023 to FY 2024 Increase/Decrease Statement:*** Funding decrease reflects changed requirements for evaluations, emerging technology tests, and assessments of new key management technologies developed by NSA's KMI program to protect and strengthen the Army Unified Network posture in FY 2023.			
Accomplishments/Planned Programs Subtotals	6.937	7.816	7.035

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
• DV5: *Crypto Modernization (Crypto Mod)*	7.756	8.370	8.288	-	8.288	8.337	8.346	8.435	8.530	Continuing	Continuing
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	47.990	50.151	87.423	-	87.423	56.273	56.459	56.486	56.062	0.000	410.844
• BS9716: *NON PEO-SPARES*	3.596	4.014	3.667	-	3.667	3.986	4.000	4.003	4.006	0.000	27.272

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 2024 Army			Date: March 2023
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 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Engineering Support (CIO/G-6)	C/FP	CACI : APG, MD	22.720	5.020	Oct 2021	3.600	Oct 2022	3.856	Oct 2023	-		3.856	0.000	35.196	-
System Engineering (CIO/G-6)	SS/LH	AFC C5ISR : APG, MD	12.786	1.473	Oct 2021	2.345	Oct 2022	2.575	Oct 2023	-		2.575	0.000	19.179	-
Engineering Support (CIO/G-6)	C/CPFF	booz Allen Hamiton : APG, MD	12.115	-		1.480	Oct 2022	0.604	Oct 2023	-		0.604	0.000	14.199	-
Service (CIO-G-6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	8.030	0.444	Oct 2021	0.391	Oct 2022	-		-		-	0.000	8.865	-
		Subtotal	55.651	6.937		7.816		7.035		-		7.035	0.000	77.439	N/A

	Prior Years	FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	55.651	6.937		7.816		7.035		-		7.035	0.000	77.439	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2024 Army		Date: March 2023
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

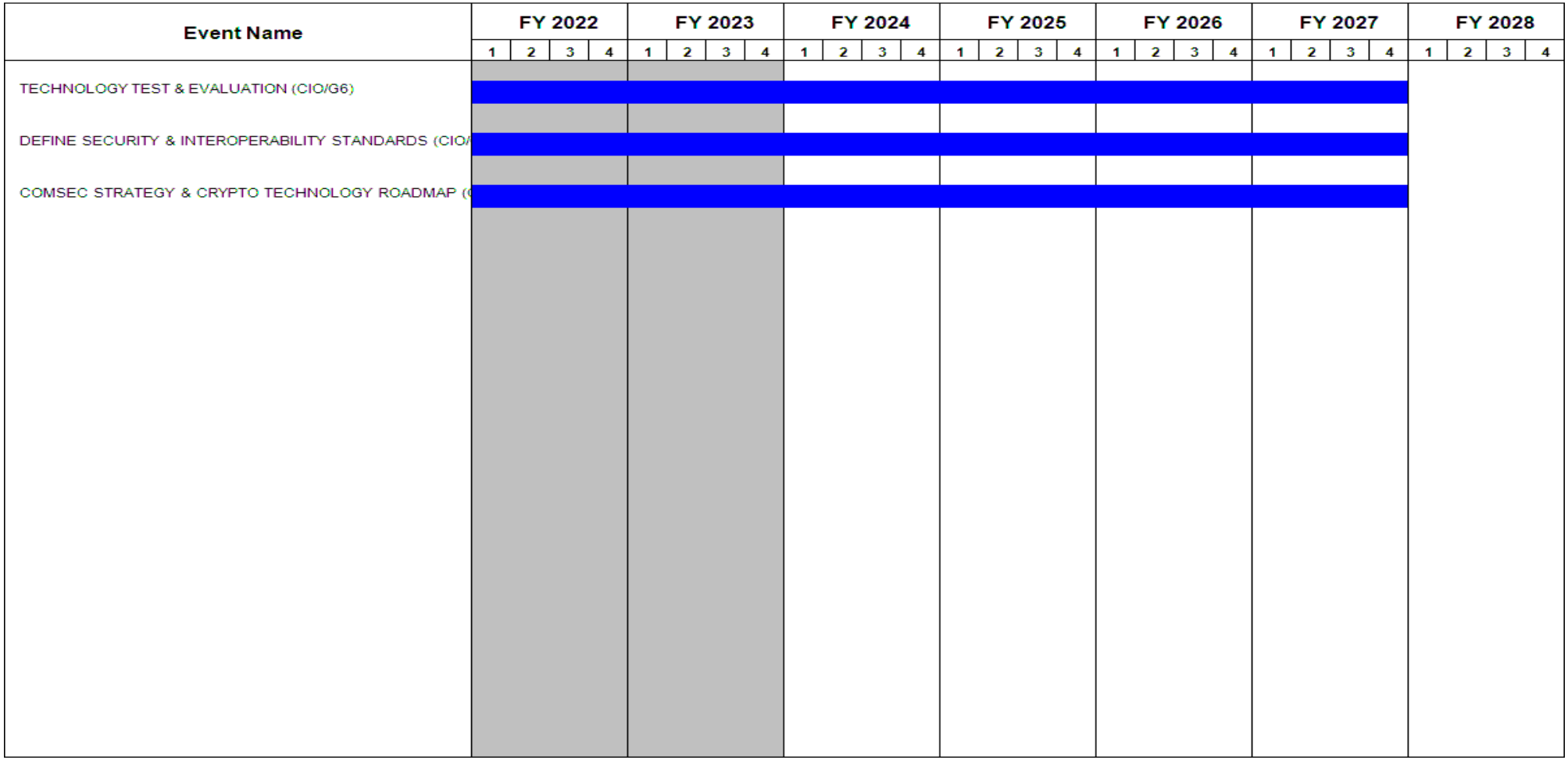

Exhibit R-4A, RDT&E Schedule Details: PB 2024 Army		Date: March 2023
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

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 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
DV4: *Key Management Infrastructure (KMI)*	-	0.987	1.023	-	-	-	1.407	1.409	1.425	1.441	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.

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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Title: Reprogrammable Cryptographic Chip Development and Evaluation	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. This effort creates a government owned potential universal cryptographic chip enabling the Army to decrease costs for encryption devices. ***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 2023 to FY 2024 Increase/Decrease Statement:*** Project DV4 has no funding request in FY 2024 due to realignment from PE 0303140A Information Systems Security Project, Project DV4: Key Management Infrastructure to PE 0605144A, Next Generation Load Device - Medium, Project BY6: Key Management Infrastructure Development.			
Accomplishments/Planned Programs Subtotals	0.987	1.023	-

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
• B96004: *KEY MANAGEMENT INFRASTRUCTURE*	78.283	75.541	72.289	-	72.289	31.524	31.699	28.697	24.050	0.000	342.083

Remarks

Line Item & Title:
B96004: Key Management Infrastructure (OPA2)

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) acquisition strategy consisted 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 allows 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).

Exhibit R-3, RDT&E Project Cost Analysis: PB 2024 Army			Date: March 2023
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)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 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	16.532	0.987	Jul 2022	1.023	Jul 2023	-		-		-	Continuing	Continuing	Continuing
		Subtotal	16.532	0.987		1.023		-		-		-	Continuing	Continuing	N/A

	Prior Years	FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	16.532	0.987		1.023		-		-		-	Continuing	Continuing	N/A

Remarks

Project DV4 has no funding request in FY 2024.

Exhibit R-4, RDT&E Schedule Profile: PB 2024 Army		Date: March 2023
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)*

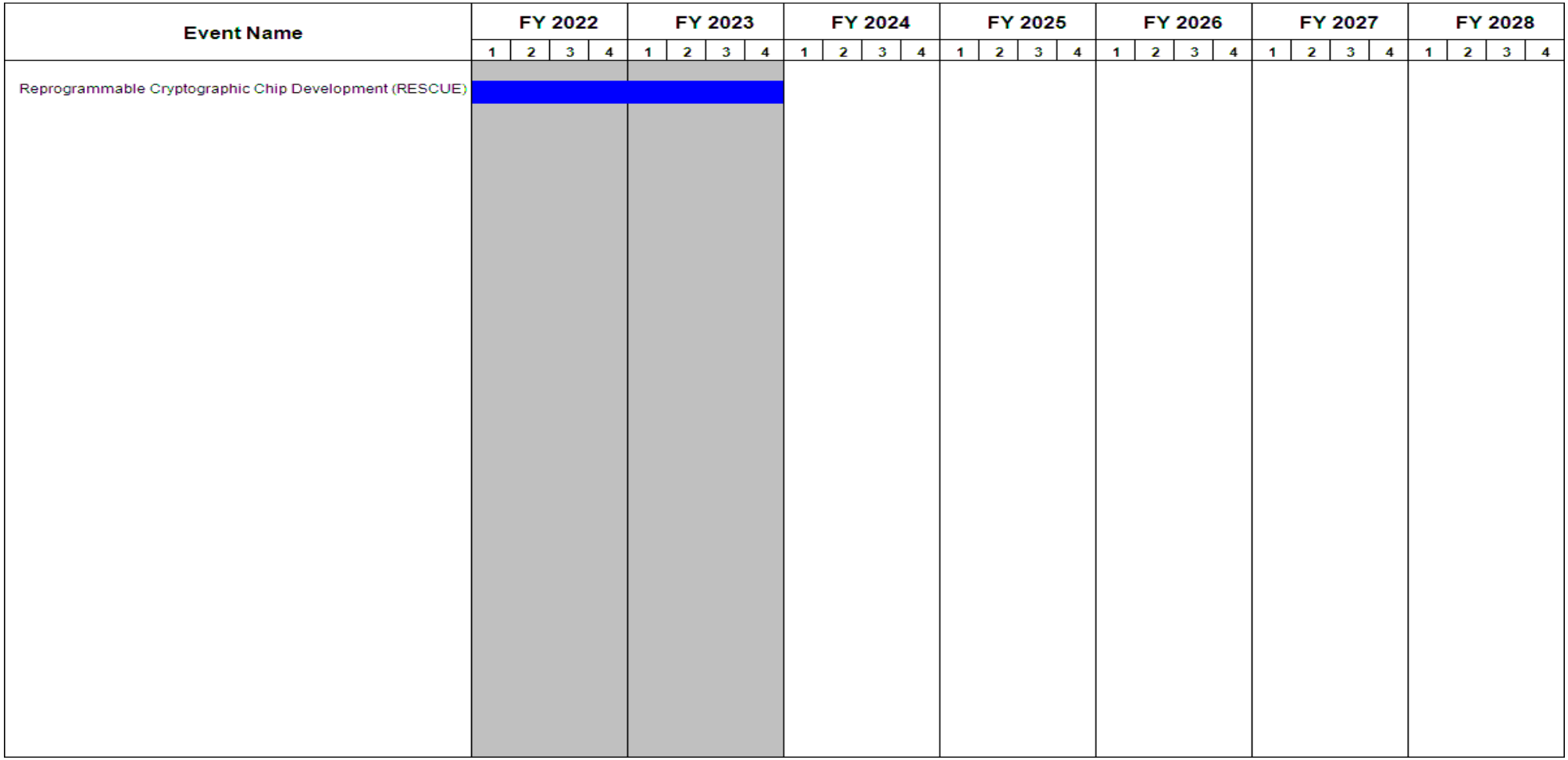

Exhibit R-4A, RDT&E Schedule Details: PB 2024 Army		Date: March 2023
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Reprogrammable Cryptographic Chip Development (RESCUE)	1	2019	4	2023

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	7.756	8.370	8.288	-	8.288	8.337	8.346	8.435	8.530	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, Cryptographic 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 2024 funds in the amount of $8.252 million 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 2022	FY 2023	FY 2024
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptographic Modernization (VACM) program	0.306	0.329	0.332

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 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 2024 Plans:*** The program continues 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 to FY 2024 Increase/Decrease Statement:*** Funding increase supports planned lifecycle of the effort.			
Title: Cryptographic Systems Test and Evaluation ***Description:*** This program supports the Army Cryptographic Modernization. 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 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	5.789	6.258	5.530

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 2024 Plans:*** Continue to conduct 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, 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), and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. These devices provide 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 2023 to FY 2024 Increase/Decrease Statement:*** The decrease is due to the reduced requirements for lab equipment.			
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 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 2024 Plans:*** 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 2023 to FY 2024 Increase/Decrease Statement:*** The increase is due to additional configuration and management development of the HAIPE in FY 2024.	1.004	1.078	1.714
Title: Program Management Office Support	0.657	0.705	0.712

Exhibit R-2A, RDT&E Project Justification: PB 2024 Army		Date: March 2023
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 2022	FY 2023	FY 2024
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 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 2024 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 2023 to FY 2024 Increase/Decrease Statement:*** Funding increase supports planned lifecycle of the effort.			
Accomplishments/Planned Programs Subtotals	7.756	8.370	8.288

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	47.990	50.151	87.423	-	87.423	56.273	56.459	56.486	56.062	0.000	410.844
• BS9716: *NON PEO-SPARES*	3.596	4.014	3.667	-	3.667	3.986	4.000	4.003	4.006	0.000	27.272

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 G-3, 15 Dec 2011 and revised and approved, 19 Jun 2015.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2024 Army			Date: March 2023
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 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Office Support	Various	PEO C3T & CECOM : Various; APG, MD	0.644	0.657	Dec 2021	0.705	Dec 2022	0.712	Dec 2023	-		0.712	0.000	2.718	Continuing
		Subtotal	0.644	0.657		0.705		0.712		-		0.712	0.000	2.718	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CCDC C5ISR S&TCD : APG, MD	7.629	1.031	Nov 2021	1.107	Nov 2022	1.086	Nov 2023	-		1.086	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	8.419	0.650	Feb 2022	0.990	Feb 2023	0.960	Feb 2024	-		0.960	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	5.177	0.272	Feb 2022	-		-		-		-	Continuing	Continuing	Continuing
		Subtotal	21.225	1.953		2.097		2.046		-		2.046	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test & Evaluation	SS/LH	CCDC C5ISR S&TCD : APG, MD	2.171	1.670	Nov 2021	1.793	Nov 2022	1.789	Nov 2023	-		1.789	0.000	7.423	-
Test & Evaluation	C/CPFF	CACI : APG, MD	7.849	3.476	Feb 2022	3.775	Feb 2023	3.741	Feb 2024	-		3.741	0.000	18.841	-
		Subtotal	10.020	5.146		5.568		5.530		-		5.530	0.000	26.264	N/A

	Prior Years	FY 2022 Cost	FY 2022 Award Date	FY 2023 Cost	FY 2023 Award Date	FY 2024 Base Cost	FY 2024 Base Award Date	FY 2024 OCO Cost	FY 2024 OCO Award Date	FY 2024 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	31.889	7.756		8.370		8.288		-		8.288	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2024 Army		Date: March 2023
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)*

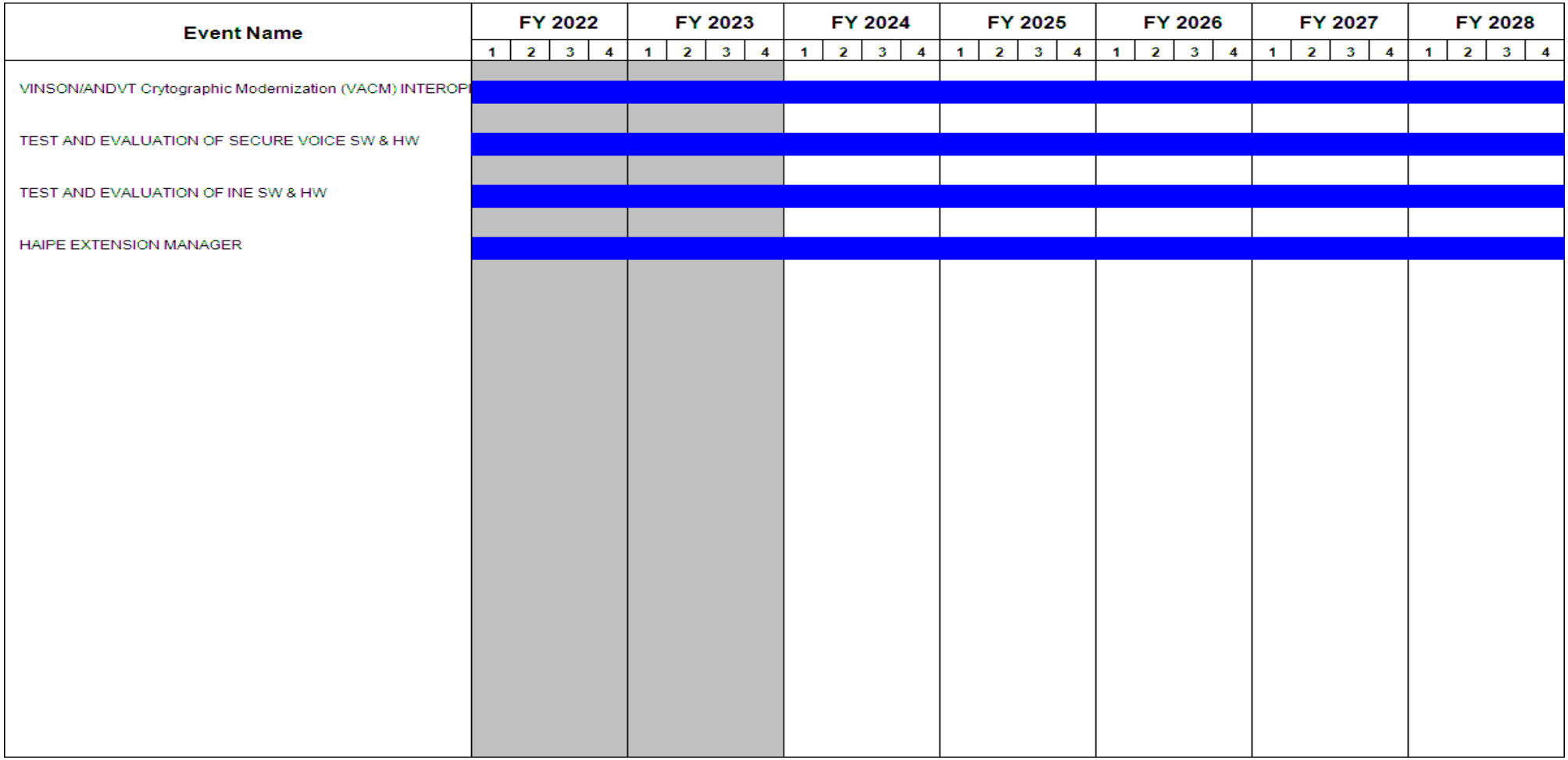

Exhibit R-4A, RDT&E Schedule Details: PB 2024 Army		Date: March 2023
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
VINSON/ANDVT Crytographic Modernization (VACM) INTEROPERABILITY	1	2016	4	2035
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