Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army											Date: February 2020	
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 2019**	**FY 2020**	**FY 2021 Base**	**FY 2021 OCO**	**FY 2021 Total**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**Cost To Complete**	**Total Cost**
Total Program Element	-	40.148	25.710	29.270	-	29.270	28.828	21.226	18.308	18.677	Continuing	Continuing
491: *Information Assurance Development*	-	9.787	8.368	8.009	-	8.009	7.596	7.638	7.593	7.993	Continuing	Continuing
DV4: *Key Management Infrastructure (KMI)*	-	2.702	11.687	13.457	-	13.457	13.339	5.408	2.475	2.398	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	5.943	5.655	7.804	-	7.804	7.893	8.180	8.240	8.286	Continuing	Continuing
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	20.745	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	20.745
FF8: *Unit Activity Monitoring (UAM)*	-	0.971	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	0.971

A. Mission Description and Budget Item Justification

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

Project 491: Army CIO/G6 manages Project 491

Project 491: Information Assurance (IA) Development supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies within the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms 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 certification and accreditation of Automation Information Systems. 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

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army	Date: February 2020
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*

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.

Project 491 FY 2021 Justification: This funding supports the continuation of providing oversight for the executions of the Army's COMSEC Modernization initiatives including major ACC updates and replacements of existing devices and systems to meet NSA mandates. Continue to support the evaluation and testing of new technologies for Army implementation in support of CM2, KMI migration and S-ICAN/ITN architecture implementation. Support efforts to provide updated end-to-end, tactical-to-strategic COMSEC standardization and implementation guidance to meet Army's operational requirements. 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. and 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. Also supports efforts to update and develop policies to posture Army's operations to implement innovative cryptographic and key management tools and services. and to participate 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.

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

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

Project DV4: The Army Key Management Infrastructure (AKMI) is the Army's implementation of the National Security Agency (NSA) KMI ACAT IAM program, automating the functions of COMSEC electronic key management, control, planning, and distribution. AKMI supports the Army's ability to communicate and distribute Cryptographic data on the Army's tactical and strategic networks by limiting adversarial access to and reducing the vulnerability of, Army Command, Control, Communications, Computers, Cyber, Intelligence (C5I) systems. AKMI devices receive, store, manage, and transfer electronic key through the network to be loaded

into communication devices such as radios and satellites to secure the network. Without this technology Warfighters are required to manually receive their cryptographic products by traveling to COMSEC account locations (which may not be co-located) and manually fill their devices.

Project DV4 FY 2021 Justification: This funding line supports COMSEC technologies within the Army with allocations for the following: $1M, 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; $12.346M to perform the systems integration and UAS development for the Next Generation Load Device - Medium (NGLD-M) to 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). This effort an Acquisition Category III (ACAT III) Program of Record (POR); $0.111M to Program Management Support, 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.

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

Project DV5 FY 2021 Justification: The program continues testing and evaluation of COMSEC devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Guidance, and new software releases to High Assurance Internet Protocol Encryptor (HAIPE) 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. The program tests interoperability and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Additionally, this program evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data.

Project ET9: Embedded Cryptographic Modernization Initiative (ECMI) program was canceled FY 2018. No FY 2021 funding is requested.

Project FF8: User activity monitoring (UAM) automation/analytics will provide technical capability to enhance Army UAM analysis effectiveness and efficiency. The UAM mission is to observe and record the actions and activities of an individual, at any time, on any device accessing Army information on classified networks in order to detect insider threats and to support authorized investigations. Army UAM is a component of the Army Insider Threat (InT) Program. Army's InT Program and UAM are

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Army	Date: February 2020
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*

conducted in accordance with the National Defense Authorization Act for Fiscal Year 2012, section 922., Insider Threat Detection; Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated 21 November 2012; Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, (Reference b) dated 7 October 2011, and Army Directive 2013-18 (Army Insider Threat Program), 31 July 2013. Innovative enhancements are required to improve UAM analysis productivity, data visualization, and workflow management. The analysis productivity objective is to develop and implement user behavior models that use UAM and other network data to identify anomalous user behavior over time, and to integrated new data sources into the UAM analytical data store and processing system. Data visualization advances will present UAM analysts behavior model processing results in an intuitive format that reduce the time required to review the results. Workflow management improvements will add new capabilities to the UAM workflow management system with the objective of enhancing analysis reporting productivity and metrics collection.

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	42.520	29.185	29.299	-	29.299
Current President's Budget	40.148	25.710	29.270	-	29.270
Total Adjustments	-2.372	-3.475	-0.029	-	-0.029
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-3.475			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-2.372	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-	-	-0.029	-	-0.029

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	9.787	8.368	8.009	-	8.009	7.596	7.638	7.593	7.993	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

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

A. Mission Description and Budget Item Justification

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

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

Develop and publish COMSEC 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, 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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
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)	9.787	8.368	8.009	-	8.009
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					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Army, coalition and Joint operating environments. This program enables the Army to collaborate and participate in Joint and Army Capability Technology Demonstrations to define, improve, develop and publish Cyber Security (CS) standards for new/modernized technology insertion to support the LWN 2025 and Beyond. This effort assesses and defines risk mitigation of CS network vulnerabilities in end-to-end Army network operations and Common Operating Environment. (CIO/G6) ***FY 2020 Plans:*** Continue to provide oversight for the executions of the Army's COMSEC Modernization initiatives. Identify and evaluate new CM, TRANSEC and KM technologies for Army implementation in support of ACC updates, KMI migration and S-ICAN/ITN architecture development. Develop end-to-end, tactical-to-strategic COMSEC standardization to meet Army?s operational requirements. Test and assess CM and KM technologies to determine the maturity and viability for Army use to protect and strengthen the Army Network posture. Document new fundamental building blocks for IA solutions, perform risk reduction testing of commercial products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Collaborate with the NSA, DoD CIO and Joint Staff to continue to support the ACC device testing and fielding. 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. Develop strategies and policies to posture Army?s operations to implement innovative cryptographic and key management tools and services. Continue to support DoD CM2 efforts. ***FY 2021 Base Plans:*** Will continue to provide oversight for the executions of the Army's COMSEC Modernization initiatives including major ACC updates and replacements of existing devices and systems. Continue to evaluate and test new technologies for Army implementation in support of CM2, KMI migration and S-ICAN/ITN architecture implementation. Continue to provide updated end-to-end, tactical-to-strategic COMSEC standardization and implementation guidance to meet Army?s operational requirements. Continue to assess new key management technologies developed by DoD joint KMI program to determine the maturity for Army fielding to protect and strengthen the Army Network posture. Continue to work with DoD CIO, NSA, DISA and other Services to resolve cryptographic interoperability issues for both embedded and standalone systems and performed risk reduction testing of commercial products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Provide timely test and evaluate results to enable					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
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 2020 to FY 2021 Increase/Decrease Statement:*** $351K decrease from FY 2020 to FY 2021.					
Accomplishments/Planned Programs Subtotals	9.787	8.368	8.009	-	8.009

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• DV5: *Crypto Modernization (Crypto Mod)*	5.943	5.655	7.804	-	7.804	7.893	8.180	8.240	8.286	Continuing	Continuing
• ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	20.745	-	0.000	-	0.000	-	-	-	-	0.000	20.745
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	26.350	66.242	81.028	0.128	81.156	52.344	52.721	52.168	65.355	0.000	396.336
• B96006: *Embedded Cryptographic Modernization*	3.520	-	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.131	3.857	3.896	-	3.896	3.935	3.936	3.996	3.996	0.000	26.747

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 2021 Army		Date: February 2020
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
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	8.629	3.734		3.500	Oct 2019	3.400	Oct 2020	-		3.400	0.000	19.263	-
System Engineering (CIO/G-6)	SS/LH	AFC C5ISR : APG, MD	6.353	3.242		2.297	Oct 2019	2.189	Oct 2020	-		2.189	0.000	14.081	-
Engineering Support (CIO/G-6)	C/CPFF	Booz Allen Hamilton : APG, MD	9.186	1.579		1.355	Oct 2019	1.350	Oct 2020	-		1.350	0.000	13.470	-
Engineering Support (CIO/G-6)	C/FFP	AASKI : Edgewood, MD	5.240	1.232		0.400	Oct 2019	0.500		-		0.500	0.000	7.372	-
Service (CIO-G-6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	7.051	-		0.816	Oct 2019	0.570	Oct 2020	-		0.570	0.000	8.437	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army		Date: February 2020
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	38.057	9.787		8.368		8.009		-		8.009	0.000	64.221	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	161.545	9.787		8.368		8.009		-		8.009	0.000	187.709	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

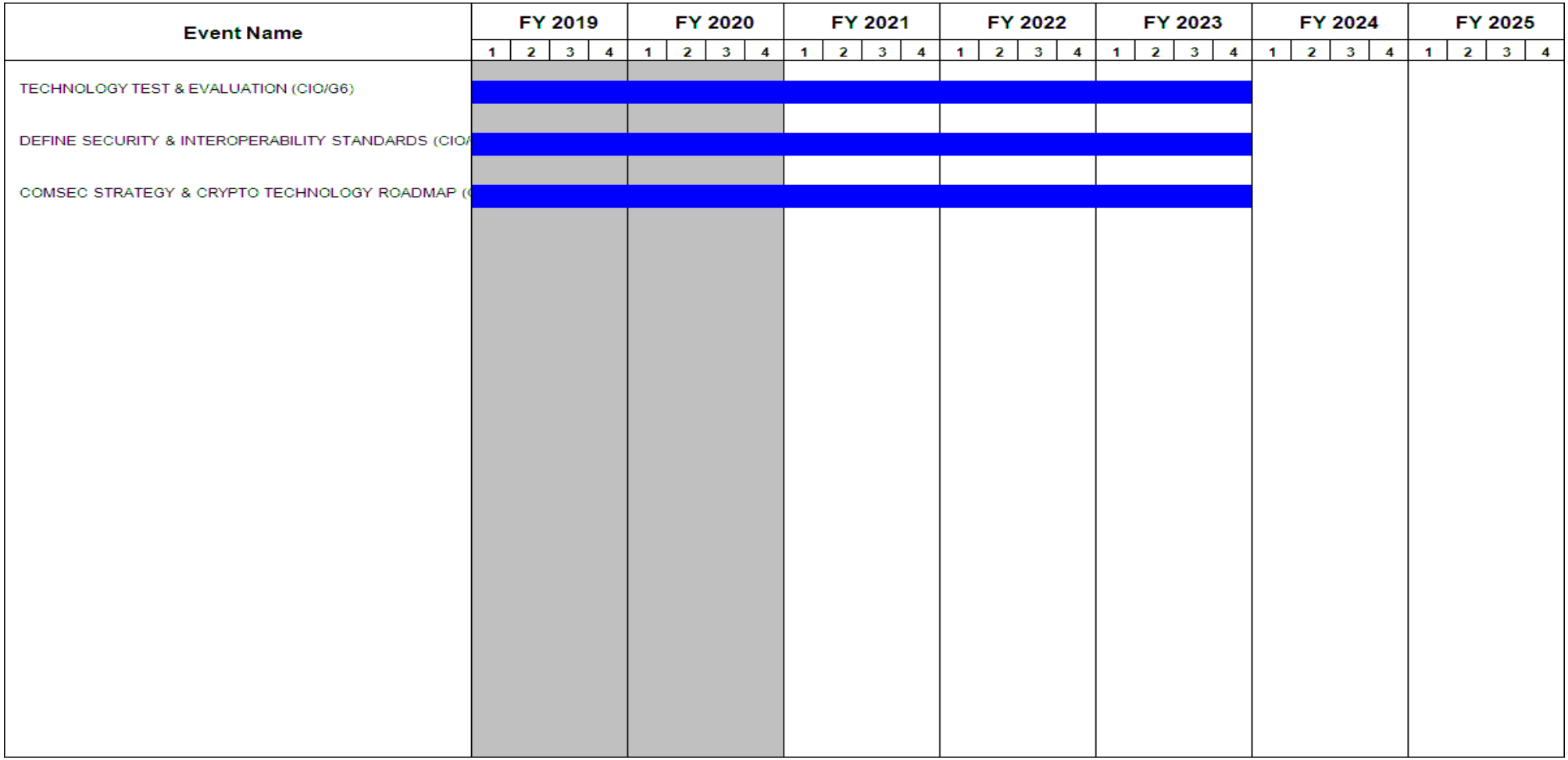

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

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	2023
DEFINE SECURITY & INTEROPERABILITY STANDARDS (CIO/G6)	1	2017	4	2023
COMSEC STRATEGY & CRYPTO TECHNOLOGY ROADMAP (CIO/G6)	1	2014	4	2023

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
DV4: *Key Management Infrastructure (KMI)*	-	2.702	11.687	13.457	-	13.457	13.339	5.408	2.475	2.398	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

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

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

As part of the Army's Key Management Infrastructure (KMI) implementation, the Next Generation Load Device - Medium (NGLD-M) is an Acquisition Category III (ACAT III) Program of Record (POR) and modernized load device that will replace approximately 144,000 legacy AN/PYQ-10A and AN/PYQ-10A(C) (Army), which is commonly referred to as the Simple Key Loader (SKL). The NGLD-M will 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. The SKL has been in the field for 14 years and does not support modernized network concepts and faces battery life attrition among early versions of the device. The NGLD-M will fulfill the current and modernized Army network concepts which will improve operational readiness, adaptiveness, and survivability of the Warfighters supporting the COMSEC requirements for approximately 1.5 million End Cryptographic Units (devices that consume cryptographic key to enable encrypted communication such as a radio or secure phone). The NGLD-M requires RDT&E investment to develop and test the hardware and software solutions to meet the operational requirements outlined in the NGLD Capability Production Document (CPD) to modernize fill devices with capability to transfer and receive cryptographic key over a network to reduce causalities and maintain mission OPTEMPO. Without this technology Warfighters are required to manually receive their cryptographic products by traveling to COMSEC account locations (which may not be co-located) and manually filling their devices.

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: Reprogrammable Cryptographic Chip Development and Evaluation	1.408	1.000	1.000	-	1.000
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					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
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 2020 Plans:*** The follow-on RESCUE technology will continue through end of FY 2020. ***FY 2021 Base 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.					
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). ***FY 2020 Plans:*** Contract Award for NGLD-M development, production, and sustainment. Conduct requirements review in preparation of System Requirements Review (SRR). Initialize development environment between Navy and Development contractor. ***FY 2021 Base Plans:*** Support NGLD-M system integration and the User Application Software (UAS) which is a graphical interface that will allow users to interact with the device. The NGLD-M development will establish configuration items and allocate system functions and performance requirements to the configurations items through a Preliminary Design Review. Further NGLD-M development will finalize the physical and functional characteristics of the NGLD-M configuration items and establish Government configuration control of the design at the Critical Design Review (CDR). At CDR, The Government will receive pre-production development models to support Highly Accelerated Life Testing for system reliability testing, End Cryptographic Unit interoperability testing, and the Risk Management Framework Security Control Assessment. ***FY 2020 to FY 2021 Increase/Decrease Statement:***	-	10.578	12.346	-	12.346

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
FY 2021 increase of $1.768M to provide for a full 12 months of support for increased requirements to deliver pre-production development models.					
Title: Acquisition Planning and Risk Mitigation ***Description:*** The Milestone Decision Authority issued a Materiel Development Decision (MDD) Acquisition Decision Memorandum (ADM) on 14 March 2019 that authorized execution of FY 2019 RDT&E funds for acquisition planning and risk mitigation. The Naval Information Warfare Systems Command (NAVWARSYSCOM) will be conducting requirements analysis for the System Requirements Document (SRD); completing traceability of requirements from the Capability Production Document (CPD) to the SRD to software functionality; defining software architecture from the derived requirements and soliciting user feedback on software workflows in order to ensure a seamless transition into development with the contract award in FY 2020.	1.250	-	-	-	-
Title: Program Management Support ***Description:*** PMO costs will be covered by OMA funding. This funds a matrixed Acquisition Program Manager (APM) from Combat Capabilities Development Command (CCDC) Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to manage the NGLD-M development effort. ***FY 2020 Plans:*** FY 2020 funds a matrixed Acquisition Program Manager (APM) from Combat Capabilities Development Command (CCDC) Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to manage the NGLD-M development effort. ***FY 2021 Base Plans:*** FY 2021 funds a matrixed Acquisition Program Manager (APM) from Combat Capabilities Development Command (CCDC) Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to manage the NGLD-M development effort. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Increase of $.002 due to inflation.	-	0.109	0.111	-	0.111
Title: FY 2018 NDAA SEC 825 MDAP Cost Overrun ***Description:*** FY 2018 NDAA SEC 825 MDAP Cost Overrun	0.044	-	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Accomplishments/Planned Programs Subtotals	2.702	11.687	13.457	-	13.457

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• B96004: *KEY MANAGEMENT INFRASTRUCTURE*	35.710	80.855	78.244	-	78.244	79.690	93.560	96.484	97.115	0.000	561.658
• OMA - 153140: *ISSP (TSEC-AKMS)*	-	-	-	-	-	-	-	-	-		

Remarks

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

D. Acquisition Strategy

Aspects of the Next Generation Load Device - Medium (NGLD-M) may include commercially availability solutions and/or interfaces, but development is required to integrate these solutions into a device that meets the rigors of NSA Type 1 certification and the Capability Production Document (CPD) requirements. There is no commercially driven market for Type-1 certified load devices that meet the requirements identified in the NGLD Family CPD. These requirements ensure secure communications by requiring the NGLD-M to provide specific tamper protections, limit electromagnetic radiation to prevent adversarial detection of the system, among others outlined within the Information Assurance Security Requirements Document. The NGLD-M acquisition also supports organic development of the User Application Software to reduce the life-cycle sustainment for the system.

Army Key Management Infrastructure (AKMI) consists of Programs of Record (POR) as well as Non PORs under Project Lead Network Enablers (PL Net E). 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.

AKMI initial Army Acquisition Program Baseline (APB) was approved 2QFY12. The AKMI Program will include the Management Clients (MGC) nodes, Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family.

The NGLD family of devices will become the primary Army Tier 3 component of the AKMI Program. The NGLD CPD calls for a family of 3 devices (small, medium and large) to meet the AKMI requirements. The AKMI program has partnered with Combat Capabilities Development Command (CCDC) Command, Control, Computers,

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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)*

Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center to develop a KMI compliant cryptographic engine, the government owner Reprogrammable Single Chip Universal Encryptor (RESCUE) that can be utilized by NGLD-M or other COMSEC devices. The NGLD-M will undergo full-and-open competition for development, production, and sustainment with a projected FY20 award. NGLD-M development will be conducted during FY19-22 culminating in NSA certification and an operational event.

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 Fiscal Year 2019 RDT&E funds for acquisition planning and risk mitigation.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
KMI Awareness (RESCUE Development and NSA Certification	C/CPFF	Dynamics Research Corporation/Engility : APG, MD	13.037	1.408	Nov 2018	1.000	Jul 2020	1.000	Jul 2021	-		1.000	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CCDC C5ISR, S&TCD : APG, MD	1.451	-		-		-		-		-	0.000	1.451	-
NGLD Development	C/CPFF	CCDC C5ISR S&TCD; NAVWARSYSCOM : APG, MD; San Diego, CA; TBD	-	1.250		10.578	Nov 2019	12.346	Nov 2020	-		12.346	Continuing	Continuing	Continuing
		Subtotal	14.488	2.658		11.578		13.346		-		13.346	Continuing	Continuing	N/A

Support ($ in Millions)

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

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	14.488	2.702		11.687		13.457		-		13.457	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
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)*

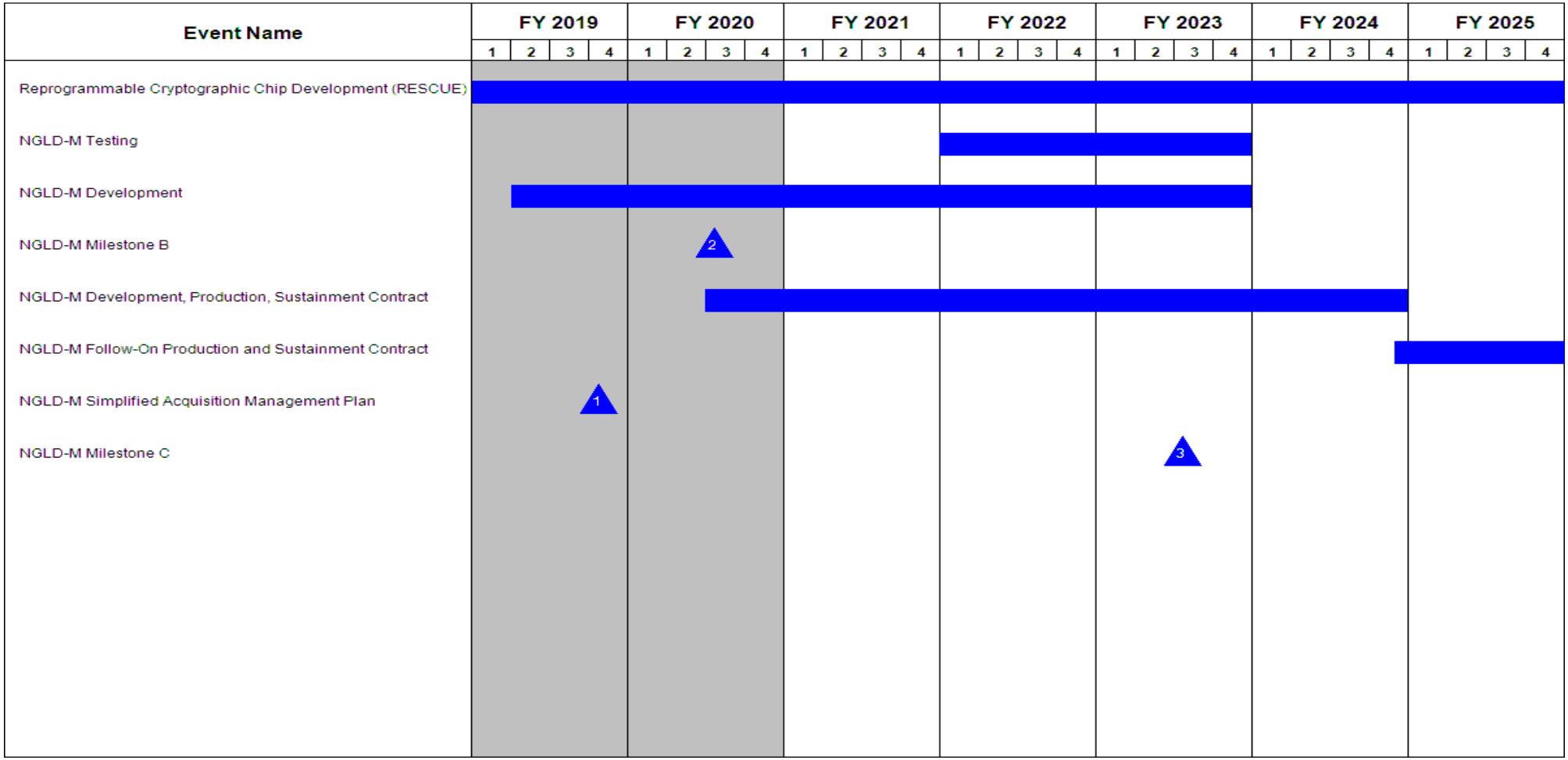

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Reprogrammable Cryptographic Chip Development (RESCUE)	1	2019	4	2026
NGLD-M Testing	1	2022	4	2023
NGLD-M Development	2	2019	4	2023
NGLD-M Milestone B	3	2020	3	2020
NGLD-M Development, Production, Sustainment Contract	3	2020	4	2024
NGLD-M Follow-On Production and Sustainment Contract	4	2024	4	2028
NGLD-M Simplified Acquisition Management Plan	4	2019	4	2019
NGLD-M Milestone C	3	2023	3	2023

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	5.943	5.655	7.804	-	7.804	7.893	8.180	8.240	8.286	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

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

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

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.625	0.746	0.300	-	0.300
Description: This program researches, assesses, tests, plans and works to integrate VACM products for the Army. These are a critical voice communications asset utilized for the president's air wing. The VACM program is a NSA mandated program established to replace legacy external cryptographic devices such as the KY-57, KY-99A, KY-58, KY-99, KY-100 and CV- 3591 / KYV-5. In order to ensure the confidentiality, integrity and availability of classified communications, the cryptographic modules must be tested for interoperability and					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
form fit to ensure a successful fielding. Each software release will require testing to insure comparability and interoperability. ***FY 2020 Plans:*** The program will continue to test and evaluate any engineering changes to Full Rate Production (FRP) of VACM devices to confirm continued capability and interoperability on Army networks and tactical systems as well as identifying new risk areas for compliance with COMSEC regulations and procedures. The program will continue fielding, performing site surveys and installing at both CONUS and OCONUS locations. ***FY 2021 Base 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 2020 to FY 2021 Increase/Decrease Statement:*** FY 2021 decrease of $.446M due to the completion of FRP testing in FY 2020.					
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 2020 Plans:*** The program will continue the 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, CHVP, CSfC Guidance, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated 16 October 2008. 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	4.372	3.944	6.520	-	6.520

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2021 Base Plans:*** Conduct testing and evaluation of COMSEC devices Link Encryptor Family (LEF), In-Line Network Encryptor (INE), Secure Voice (SV) to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures, with particular emphasis on the Advanced Cryptographic Capabilities (ACC) program lead by the NSA. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Guidance and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Revision dated 8 June 2018. These devices provides the critical security backbone for all NIPRNET, SIPRNET, JWICS and Intelligence networks in both the Tactical and Enterprise networks. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure to defend against adversary attack and exploitation. The program tests interoperability and provides ways to insert data at rest (DAR) and data in transit (DIT) technology within the existing and future network infrastructure. Additionally, this program evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** FY 2021 increase of $2.576M due to the Advanced Cryptographic Capabilities (ACC) effort phases 2 and 3 which increases the amount of test & evaluation from 5 to 8 devices (KG 245AIX, KIV 7M, STE, KSV 21, KG 250, Ectocrypt Black, Talon 2 and Iridium Follow-On Secure Handset (FOSH)). The Army must comply with National Security ACC policy as managed by NSA to allow for communication of classified information.					
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 2020 Plans:*** 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	0.946	0.965	0.984	-	0.984

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
HAIPE extensions. This will facilitate the upgrade of the Army HAIPIES to include new cyber sensor functionality for the tactical cell. ***FY 2021 Base 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 2020 to FY 2021 Increase/Decrease Statement:*** FY 2021 increase of $.019 due to inflation.					
Accomplishments/Planned Programs Subtotals	5.943	5.655	7.804	-	7.804

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	9.787	8.368	8.009	-	8.009	7.596	7.638	7.593	7.993	Continuing	Continuing
• ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	20.745	-	0.000	-	0.000	-	-	-	-	0.000	20.745
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	26.350	66.242	81.028	0.128	81.156	52.344	52.721	52.168	65.355	0.000	396.336
• B96006: *Embedded Cryptographic Modernization*	3.520	-	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.131	3.857	3.896	-	3.896	3.935	3.936	3.996	3.996	0.000	26.747

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by CIO/G6 and PL ES-CYBER
ET9 - Embedded Crypto Modernization - RDTE
B96002 - Cryptographic Systems - OPA2
B96006 - Embedded Cryptographic Modernization - OPA2
BS9716 - NON PEO-SPARES - OPA4

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
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)*

D. Acquisition Strategy

The Cryptographic Systems program integrates and validates hardware and software solutions to provide COMSEC superiority in order to protect against threats, increase battlefield survivability/lethality, and enable critical Mission Command activities. The objective of the Crypto Mod program is to provide adaptive, flexible, and programmable cryptographic systems using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic systems. To support this objective, the Cryptographic Systems Program utilizes NSA contracts in order to procure devices. All existing and emerging encryptors are then tested and evaluated for Functionality, Security, Interoperability, and backward compatibility on software and hardware for both Tactical and Enterprise systems and assessments of new software and hardware updates to end user devices and software to ensure they remain hardened against cyber-attack. The effort will support the network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating networked vulnerabilities to Army information security systems. 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 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CCDC C5ISR S&TCD : APG, MD	5.583	0.510	Nov 2018	0.525	Nov 2019	0.540	Nov 2020	-		0.540	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	6.641	0.801	Feb 2019	0.340	Feb 2020	0.310	Feb 2021	-		0.310	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	4.332	-		0.578	Feb 2020	0.234	Feb 2021	-		0.234	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	5.306	0.260	Apr 2019	0.268	Apr 2020	0.200	Apr 2021	-		0.200	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	60.598	1.571		1.711		1.284		-		1.284	Continuing	Continuing	N/A

Remarks

$2.000M in FY19 funding was returned to the PEO mid-year as excess. FY18 funding originally turned in for recission was partially returned to CS late FY18 and was utilized to pay CCDC C5ISR S&TCD labor in FY19, resulting in the $2.000M excess FY19 funding being returned. FY21 Plan: No planned excess funding for FY21
Envision, Aberdeen, Maryland is a subcontractor under CACI; FY19 and FY21 funding is captured on the CACI line.
Embedded Crypto Modernization Support was cancelled.

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test & Evaluation	SS/LH	CCDC C5ISR S&TCD : APG, MD	-	0.262	Nov 2018	0.272	Nov 2019	1.300	Nov 2020	-		1.300	0.000	1.834	-
Test & Evaluation	C/CPFF	CACI : APG, MD	-	2.485	Feb 2019	1.756	Feb 2020	1.800	Feb 2021	-		1.800	0.000	6.041	-
Test & Evaluation	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	-	0.985	Feb 2019	1.057	Feb 2020	1.820	Feb 2021	-		1.820	0.000	3.862	-
Test & Evaluation	C/CPFF	AASKI : APG, MD	-	0.640	Apr 2019	0.859	Apr 2020	1.600	Apr 2021	-		1.600	0.000	3.099	-
		Subtotal	-	4.372		3.944		6.520		-		6.520	0.000	14.836	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	60.598	5.943		5.655		7.804		-		7.804	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
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)*

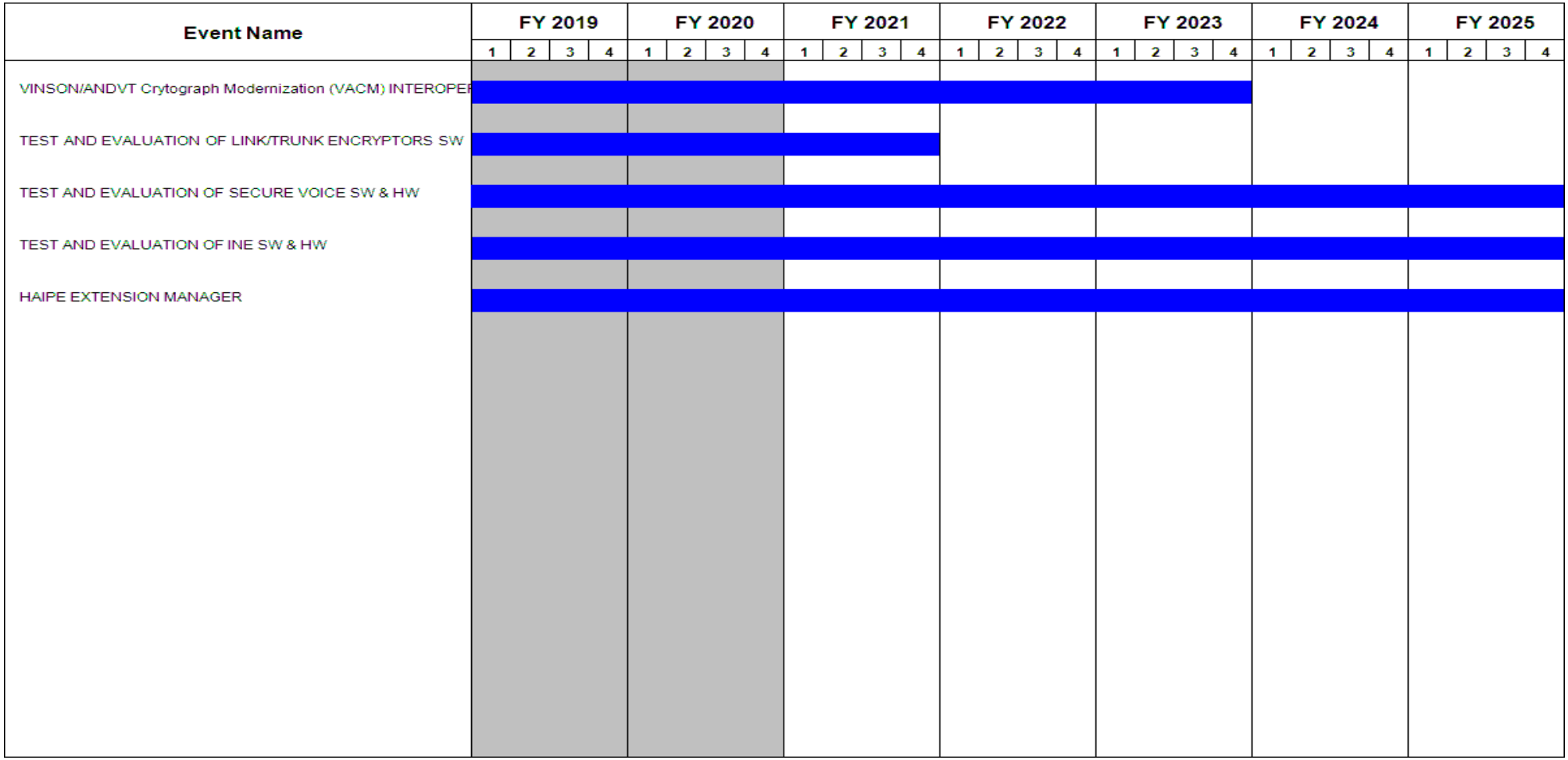

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

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	2025
TEST AND EVALUATION OF INE SW & HW	1	2017	4	2025
HAIPE EXTENSION MANAGER	1	2017	4	2025

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	20.745	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	20.745
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Project ET9, Embedded Crypto Modernization (Crypto Mod) supports the Army's Network Modernization Strategy Lines of Effort (LOE) 1 Network Enablers Functions.

Modernize the AN/ARC-201D Single Channel Ground and Airborne Radio Systems (SINCGARS) to meet CJCSI mandated cryptographic requirements through the execution of an engineering change effort to provide a bridging radio solution for Army Aviation rotary wing platforms. Support the Unified Network key near term imperative of achieving air-ground integration. Crypto modernization will ensure compliance with Key Management Infrastructure (KMI), add algorithms that address cyber vulnerabilities, improve 'secure but unclassified' network support, and provide better support to coalition interoperability.

Embedded Cryptographic Modernization Initiative (ECMI) is an upgrade activity that will ensure Army radios remain secure by operating with modern cryptographic algorithms. Tactical radios using legacy embedded cryptographic systems will no longer be able to communicate securely after cease key dates documented in the Chairman of the Joint Chiefs Staff instruction (CJCSI) 6510. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army tactical radios are required to support modern cryptographic capabilities by implementing modern algorithms. If cease key dates are not met, the Army will be forced to communicate at risk.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: FY19 Rescission	20.745	-	-	-	-
Accomplishments/Planned Programs Subtotals	20.745	-	-	-	-

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	9.787	8.368	8.009	-	8.009	7.596	7.638	7.593	7.993	Continuing	Continuing
• DV5: *Crypto Modernization (Crypto Mod)*	5.943	5.655	7.804	-	7.804	7.893	8.180	8.240	8.286	Continuing	Continuing
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	26.350	66.242	81.028	0.128	81.156	52.344	52.721	52.168	65.355	0.000	396.336

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*	

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• B96006: *Embedded Cryptographic Modernization*	3.520	-	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.131	3.857	3.896	-	3.896	3.935	3.936	3.996	3.996	0.000	26.747

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by PL Net E, CIO/G6 and PL ES-CYBER
DV5 - Crypto Modernization - RDTE
B96002 - Cryptographic Systems - OPA2
B96006 - Embedded Cryptographic Modernization - OPA2
BS9716 - NON PEO-SPARES - OPA4

D. Acquisition Strategy

The objective of the ECMI program is to provide adaptive, flexible, and programmable embedded cryptographic solutions using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic tactical radios. ECMI will design, develop, and execute upgrade activities to ensure non modernized Army tactical radios will be able to accept and utilize modern cryptographic algorithms.

Applicable documents affecting Tactical Radio ONS, ORD, & CPDs requiring crypto:
CDD for Cryptographic Equipment and Services Modernization, Increment 1, dated March 2010.
CJCSI 6510.02E - "Cryptographic Modernization Planning", 01 April 2014.
CNSSP-15 - "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems", 01 October 2012.
NSA CSS 3-9 - "Cryptographic Modernization Initiative Requirements for Type 1 Cryptographic Products", dated 28 March 2013.
Memorandum from Army Acquisition Executive with subject "Management and Procurement of Communications Security (COMSEC) Capability, dated 28 Feb 2012.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
AMF-ARC-201D Crypto Mod - SE/PM	TBD	TBD : TBD	1.639	-		-		-		-		-	0.000	1.639	-
		Subtotal	1.639	-		-		-		-		-	0.000	1.639	N/A

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PM TR Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	7.953	1.037		-		-		-		-	0.000	8.990	-
PM TR Program Mgmt Personnel	C/CPFF	BAH : Aberdeen, MD	1.424	-		-		-		-		-	0.000	1.424	-
AMF-ARC-201D Crypto Mod - Dev Engineering & Prototyping	TBD	TBD : TBD	22.752	19.708		-		-		-		-	0.000	42.460	-
		Subtotal	32.129	20.745		-		-		-		-	0.000	52.874	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
AMF-ARC-201D Crypto Mod - Test and Evaluation	TBD	TBD : TBD	19.555	-		-		-		-		-	0.000	19.555	-
		Subtotal	19.555	-		-		-		-		-	0.000	19.555	N/A

	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	53.323	20.745		0.000		-		-		-	0.000	74.068	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

	FY 2012				FY 2013				FY 2014				FY 2015				FY 2016				FY 2017				FY 2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Market Research																												

	FY 2019				FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Market Research																												

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Market Research	1	2017	4	2018

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) FF8 / *Unit Activity Monitoring (UAM)*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
FF8: *Unit Activity Monitoring (UAM)*	-	0.971	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	0.971
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

User activity monitoring (UAM) automation/analytics will provide technical capability to enhance Army UAM analysis effectiveness and efficiency. The UAM mission is to observe and record the actions and activities of an individual, at any time, on any device accessing Army information on classified networks in order to detect insider threats and to support authorized investigations. Army UAM is a component of the Army Insider Threat (InT) Program. Army's InT Program and UAM are conducted in accordance with the National Defense Authorization Act for FY 2012, section 922., Insider Threat Detection; Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated 21 November 2012; Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, (Reference b) dated 7 October 2011, and Army Directive 2013-18 (Army Insider Threat Program), 31 July 2013. Innovative enhancements are required to improve UAM analysis productivity, data visualization, and workflow management. The analysis productivity objective is to develop and implement user behavior models that use UAM and other network data to identify anomalous user behavior over time, and to integrated new data sources into the UAM analytical data store and processing system. Data visualization advances will present UAM analysts behavior model processing results in an intuitive format that reduce the time required to review the results. Workflow management improvements will add new capabilities to the UAM workflow management system with the objective of enhancing analysis reporting productivity and metrics collection.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: Unit Activity Monitoring ***Description:*** FY 2019 Base funds in the total amount of $.971 million are provided for software engineering development and testing resources to enhance the Army? UAM data processing, analysis, and data visualization capabilities, and its workflow management system, plus the integration of new data sources into the data processing component. All work is focused on the development of new capabilities. The details of this program are reported in accordance with Title 10, United States Code, Section 119(a)(1).	0.971	-	-	-	-
Accomplishments/Planned Programs Subtotals	0.971	-	-	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

D. Acquisition Strategy

FY 2019: The planned acquisition strategy to acquire UAM Automation/Analytics software engineering services is to award through the use of competitive acquisition, a Base plus three-option year firm-fixed price contract.

FY 2019: The planned acquisition is to exercise next option year of the software engineering services contract.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Army			Date: February 2020
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) FF8 / *Unit Activity Monitoring (UAM)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Engineering Development	C/TBD	TBD : TBD	19.491	0.971	Jun 2019	-		-		-		-	0.000	20.462	Continuing
		Subtotal	19.491	0.971		-		-		-		-	0.000	20.462	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	19.491	0.971		0.000		-		-		-	0.000	20.462	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

	FY 2012				FY 2013				FY 2014				FY 2015				FY 2016				FY 2017				FY 2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Contract Award																											■	

	FY 2019				FY 2020				FY 2021				FY 2022				FY 2023				FY 2024				FY 2025			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Contract Award																												

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Army		Date: February 2020
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Contract Award	3	2018	3	2018