Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Army	**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	108.755	42.520	29.185	-	29.185	29.299	28.855	21.245	17.125	Continuing	Continuing
491: *Information Assurance Development*	-	9.787	10.159	8.368	-	8.368	8.017	7.604	7.645	5.600	0.000	57.180
DV4: *Key Management Infrastructure (KMI)*	-	4.508	2.702	13.187	-	13.187	13.470	13.351	3.413	3.477	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	26.055	7.943	7.630	-	7.630	7.812	7.900	10.187	8.048	Continuing	Continuing
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	48.914	20.745	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	69.659
FF8: *Unit Activity Monitoring (UAM)*	-	19.491	0.971	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	20.462

A. Mission Description and Budget Item Justification

The Information Systems Security Program funding line supports the Army's Network Modernization Strategy Line of Effort (LOE) 1, Unified Network.

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 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 2020 Army	**Date:** March 2019
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 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. The Army's Mission Command Network Modernization implementation Plan, date 17 April 2018, states that LOE 1 to be a Unified Network which includes the attributes of being, "Protected, Resilient, Survivable" (p. 11) COMSEC is the Army's implementation of NSA protections to achieve LOE 1.

Project DV4: The Army Key Management Infrastructure (AKMI) is the Army's implementation of the 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, Intelligence (C4I) systems. The AKMI System of Systems (SoS) systems components are the Management Client (MGC), Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family of fill devices. The AKMS SoS components are the Local COMSEC Management Software (LCMS), ACES, and Simple Key Loader (SKL).

Project DV5: The Army COMSEC program supports using NSA developed COMSEC technologies within the Army providing encryption, trusted software, or standard operating procedures, and integrating these mechanisms into National Security Systems (NSS), and National Security Information (NSI)systems in support of securing the Army network (which is made up of 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 emerging 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 SPG and the AMSP.

Project ET9: Embedded Cryptographic Modernization Initiative (ECMI) program was cancelled FY 2018. No FY 2020 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 conducted in accordance with the National Defense Authorization Act for Fiscal Year 2012, section 922., Insider Threat Detection; Presidential Memorandum, National

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army		Date: March 2019
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*	

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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	132.438	68.533	54.714	-	54.714
Current President's Budget	108.755	42.520	29.185	-	29.185
Total Adjustments	-23.683	-26.013	-25.529	-	-25.529
• Congressional General Reductions	-0.074	-0.013			
• Congressional Directed Reductions	-38.000	-26.000			
• Congressional Rescissions	-	-			
• Congressional Adds	18.000	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-3.609	-			
• Adjustments to Budget Years	-	-	-25.529	-	-25.529

Change Summary Explanation

FY 2020 funding is reduced by $25.529 million due to the cancellation of the Embedded Cryptographic Modernization Initiative (ECMI) program.
FY 2019 Congressional Reduction of $26.000 million for program delay ($25.000 million) and crypto modernization inaccurate contract awards ($1.000 million).
FY 2018 Congressional Reduction of $38.000 million for excess growth (13.000 million) and excess embedded crypto modernization funding due to program delay ($25.000 million); Congressional Add of $18.000 million for Cybersecurity operations center.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	9.787	10.159	8.368	-	8.368	8.017	7.604	7.645	5.600	0.000	57.180
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

PE 0303140A, project 491 includes funding for the Army CIO/G6, Project Lead (PL) Network Enablers (Net E), 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 the 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.

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 provides situational awareness of the cyberspace battlefield. It provides the computer network defense provider with a 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.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
Title: Assessing emerging COMSEC hardware and software systems and products (PL Net E) ***Description:*** Conduct research and analyses as well as basic testing for meeting specific focused goals that will enhance the functions and support of cryptographic systems improving the security and usability of the Army tactical and enterprise networks. (PL Net E)	1.466	-	-
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) ***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 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 2019 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 2020 Plans:*** Will 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	8.321	9.787	8.368

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
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 2019 to FY 2020 Increase/Decrease Statement:*** The decrease from FY 2019 to FY 2020 is in direct support to test and evaluate the maturity of Army's CM devices to meet the ACC standards to provide the Warfighter with the ability to secure, maintain compliance, interoperability and protect National Information. The CM effort will employ common standards and technologies to reduce redundancies and maximize scalable solutions that can respond to cyber threats, mission changes and interoperability. This is IAW the Army Communications Security (COMSEC) Modernization Implementation Planning Guidance FY 2019/2020.			
Title: FY 2019 SBIR / STTR Transfer ***Description:*** FY 2019 SBIR / STTR Transfer ***FY 2019 Plans:*** FY 2019 SBIR / STTR Transfer ***FY 2019 to FY 2020 Increase/Decrease Statement:*** FY 2019 SBIR / STTR Transfer	-	0.372	-
Accomplishments/Planned Programs Subtotals	9.787	10.159	8.368

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• DV5: *Crypto Modernization (Crypto Mod)*	26.055	7.943	7.630	-	7.630	7.812	7.900	10.187	8.048	Continuing	Continuing
• ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	48.914	20.745	0.000	-	0.000	-	-	-	-	0.000	69.659

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	47.536	26.350	72.457	-	72.457	36.113	26.399	30.776	39.721	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	3.520	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.135	3.131	3.857	-	3.857	3.901	3.939	3.940	4.000	0.000	25.903

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.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
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)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PL Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	80.317	1.466		-		-		-		-	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			122.022	1.466		-		-		-		-	0.000	123.488	N/A

Test and Evaluation ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
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	6.433	2.196		3.377		3.500		-		3.500	Continuing	Continuing	-
System Engineering (CIO/G-6)	SS/LH	AFC CERDEC : APG, MD	4.857	1.496		1.682		2.297		-		2.297	Continuing	Continuing	-
Engineering Support (CIO/G-6)	C/CPFF	Booz Allen Hamilton : APG, MD	7.449	1.737		2.890		1.355		-		1.355	Continuing	Continuing	-
Engineering Support (CIO/G-6)	C/FFP	AASKI : Edgewood, MD	3.427	1.813		1.120		0.400		-		0.400	Continuing	Continuing	-
Service (CIO-G-6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	5.972	1.079		1.090		0.816		-		0.816	Continuing	Continuing	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
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 2018 Cost	FY 2018 Award Date	FY 2019 Cost	FY 2019 Award Date	FY 2020 Base Cost	FY 2020 Base Award Date	FY 2020 OCO Cost	FY 2020 OCO Award Date	FY 2020 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	29.736	8.321		10.159		8.368		-		8.368	Continuing	Continuing	N/A

	Prior Years	FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	151.758	9.787		10.159		8.368		-		8.368	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

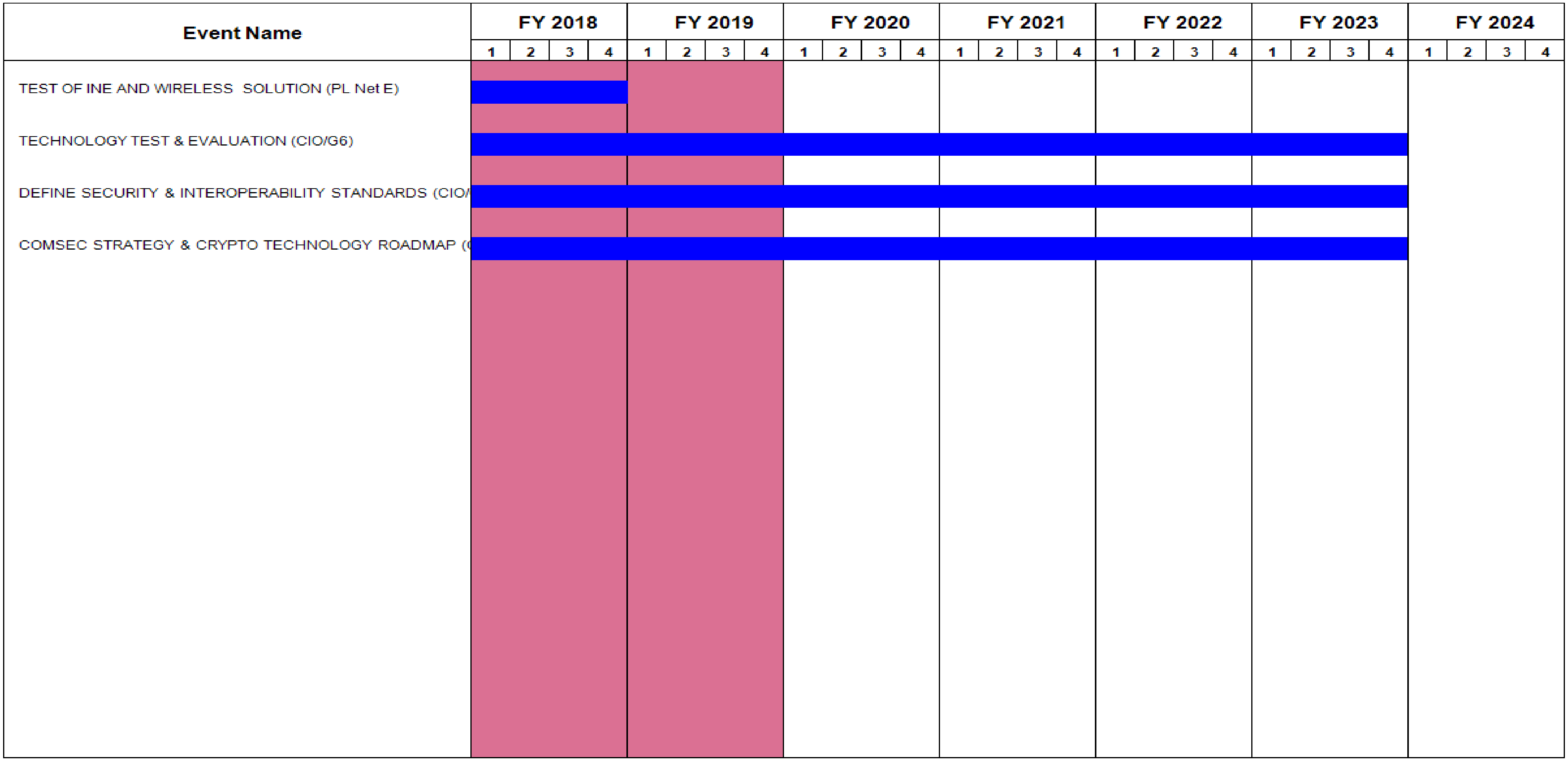

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140A **/** *Information Systems Security Program*	**Project (Number/Name)** 491 **/** *Information Assurance Development*

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 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
DV4: *Key Management Infrastructure (KMI)*	-	4.508	2.702	13.187	-	13.187	13.470	13.351	3.413	3.477	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

A. Mission Description and Budget Item Justification

Project DV4, Key Management Infrastructure (KMI) supports the Army's Network Modernization Strategy Lines of Effort (LOE) 1 Network Enablers Functions.

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 Army's Mission Command Network Modernization Implementation Plan states that LOE 1 to be a Unified Network which includes the attributes of being, "Protected, Resilient, Survivable" which Communications Security (COMSEC) is the Army's implementation of NSA protections to achieve LOE 1. KMI is foundational to the Army's Network Enabling Functions (Key Management Infrastructure).

The Army Key Management Infrastructure (AKMI) is the Army's implementation of the National Security Agency's (NSA) Key Management Infrastructure (KMI) ACAT IAM program. AKMI supports Department of Defense (DoD) Global Information Grid (GIG) Net Centric and Cryptographic Modernization Initiatives (CMI) and supports emerging requirements transitioned from the Army Key Management System (AKMS). AKMI automates the functions of Communications Security (COMSEC) electronic key management, control, planning, and distribution. AKMI supports the Army's ability to communicate and distribute data on the Army's tactical and strategic networks by limiting adversarial access to, and reducing the vulnerability of, Army Command, Control, Communications, Computers, Intelligence (C4I) systems.

The AKMI Program includes the Management Clients (MGC) nodes, Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family of devices to include the NGLD Small, Medium and Large. AKMI provides an integrated, operational environment that brings essential key management functions in-band. Objective AKMI will leverage NSA KMI program to provide secure software provisioning, will support legacy and modern End Cryptographic Units (ECU)s, simplifies all aspects of key provisioning and ECU management with traceability to individuals, expands operations to DoD unclassified networks, North Atlantic Treaty Organization (NATO) and Coalition users, automates manual business processes to increase Soldier efficiency, transforms key delivery from manual to an automate enterprise service and will provide an Over the Network Keying (OTNK) capability to support CMI.

One of the major enhancement in the AKMI architecture is the ability to leverage the various capabilities and services from NSA KMI. The end state for the Army is to leverage AKMI capabilities (OTNK, Mission Plan/Mission Support System (MP/MSS), Delivery Only Client (DOC), Client Host Only (CHO)) to increase automation, reduce soldier oversight, manage, and deliver key products to the tactical edge up through strategic ECU's. The objective AKMI capabilities will be found in all of the products across the AKMI product line to include MGC, ACES and NGLD family of fill devices. NGLD family will be an enduring solution to bridge the gap until legacy ECUs are fully modernized.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*	

The Next Generation Load Device - Medium (NGLD-M) is scheduled to replace the AN/PYQ-10A and AN/PYQ-10A(C), Simple Key Loader (SKL). The 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). This effort is proposed as an Acquisition Category III (ACAT III). Program of Record (POR). Testing of this device will also require development funds and culminate in a user test during FY22.

The NGLD-Medium (NGLD-M) is reliant on the Reprogrammable Single Chip Universal Encryptor (RESCUE), a new KMI-compliant cryptographic engine that is currently being developed by CERDEC S&TCD. This product culminates in a government owned technical data package supporting Cryptographic Modernization requirements. The NGLD-M is a key transition partner for this technology. Further uses of this product are anticipated across Army and other services require reprogrammable Cryptographic requirements. NSA certification is expected during FY19.

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020**
Title: RESCUE Development, Evaluation, and NSA Certification ***Description:*** RESCUE creates 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. Fill Devices and ECUs will receive, authenticate, and decrypt OTNK messages and increase WarFighter survivability by minimizing the need for Soldiers to travel to obtain keys. Additionally, Cryptographic Modernization decreases probability of key compromise and therefore, network survivability. Redesign and developmental efforts using modern and readily available components for use in the Army's Next Generation Load Devices (NGLDs) are currently underway. NGLD ? M will also address requirements codified in the NGLD CPD and the AKMI CPD that were technologically unachievable with the legacy KOV 21 card as used in the Army?s SKL. ***FY 2019 Plans:*** The follow-on RESCUE technology will continue in FY2019. ***FY 2020 Plans:*** The follow-on RESCUE technology will continue through end of FY2020. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Requirements include increased projected developmental and operational test requirement in support of NGLD-M.	4.508	2.702	3.187
Title: NGLD Medium Development and NSA Certification ***Description:*** The 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). This effort is proposed as an Acquisition Category III (ACAT III). Program of Record (POR). ***FY 2020 Plans:***	-	-	8.500

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
Contract award for development, production, and sustainment. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Requirements include updated projected developmental support for NGLD-M.			
Title: NGLD-M Test & Evaluation ***Description:*** The 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). Operational testing of this device will require development funds and culminate in a user test during FY22. ***FY 2020 Plans:*** NGLD-M test and evaluation required for development. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** NGLD-M operational test and evaluation requirements were reevaluated and adjusted.	-	-	1.500
Accomplishments/Planned Programs Subtotals	4.508	2.702	13.187

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• B96004: *KEY MANAGEMENT INFRASTRUCTURE*	56.948	35.710	88.442	-	88.442	89.912	81.432	98.363	99.012	0.000	549.819

Remarks

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

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) is a Non Program of Record (POR) 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 ~1.5M End Cryptographic Units (ECU)s necessary to communicate and distribute data on the Army's tactical and strategic networks.

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. Each component of the AKMI Program is in a different phase of the acquisition cycle.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140A **/** *Information Systems Security Program*	**Project (Number/Name)** DV4 **/** *Key Management Infrastructure (KMI)*

The NSA KMI Program is replacing the NSA Electronic Key Management System (EKMS) program. As the DoD Key Management Lead, NSA is dictating the change from EKMS to KMI by a sunset date of December 2017. Components of the AKMI Program will be retained and adapted from the legacy AKMS program while others will be developed and fielded to meet AKMI requirements.

The NGLD family of devices will become the primary Army Tier 3 component of the AKMI Program. The NGLD Capability Production Document (CPD) was signed 4QFY13. 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 RDECOM CERDEC to develop a KMI compliant cryptographic engine, the Reprogrammable Single Chip Universal Encryptor (RESCUE). The NGLD-M will undergo full-and-open competition for development, production, and sustainment during FY19 with a projected FY20 award. NGLD-M development will be conducted during FY20-22 culminating in NSA certification and an operational event. NGLD-M projects LRIP and FRP during FY22.

E. Performance Metrics

N/A

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2020 Army		**Date:** March 2019
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)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
KMI Awareness (RESCUE Development and NSA Certification	C/CPFF	Dynamics Research Corporation/Engility : APG, MD	8.529	4.508	Jul 2018	2.702	Jul 2019	3.187	Jul 2020	-		3.187	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CERDEC, S&TCD : APG, MD	1.451	-		-		-		-		-	0.000	1.451	-
NGLD Development and NSA Certification	C/CPFF	CERDEC STCD : APG, MD	-	-		-		8.500		-		8.500	Continuing	Continuing	Continuing
		Subtotal	9.980	4.508		2.702		11.687		-		11.687	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
NGLD-M Testing & Evaluation	C/CPFF	CERDEC, S&TCD : APG, MD	-	-		-		1.500		-		1.500	0.000	1.500	-
		Subtotal	-	-		-		1.500		-		1.500	0.000	1.500	N/A

	Prior Years	**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	9.980	4.508		2.702		13.187		-		13.187	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
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)*

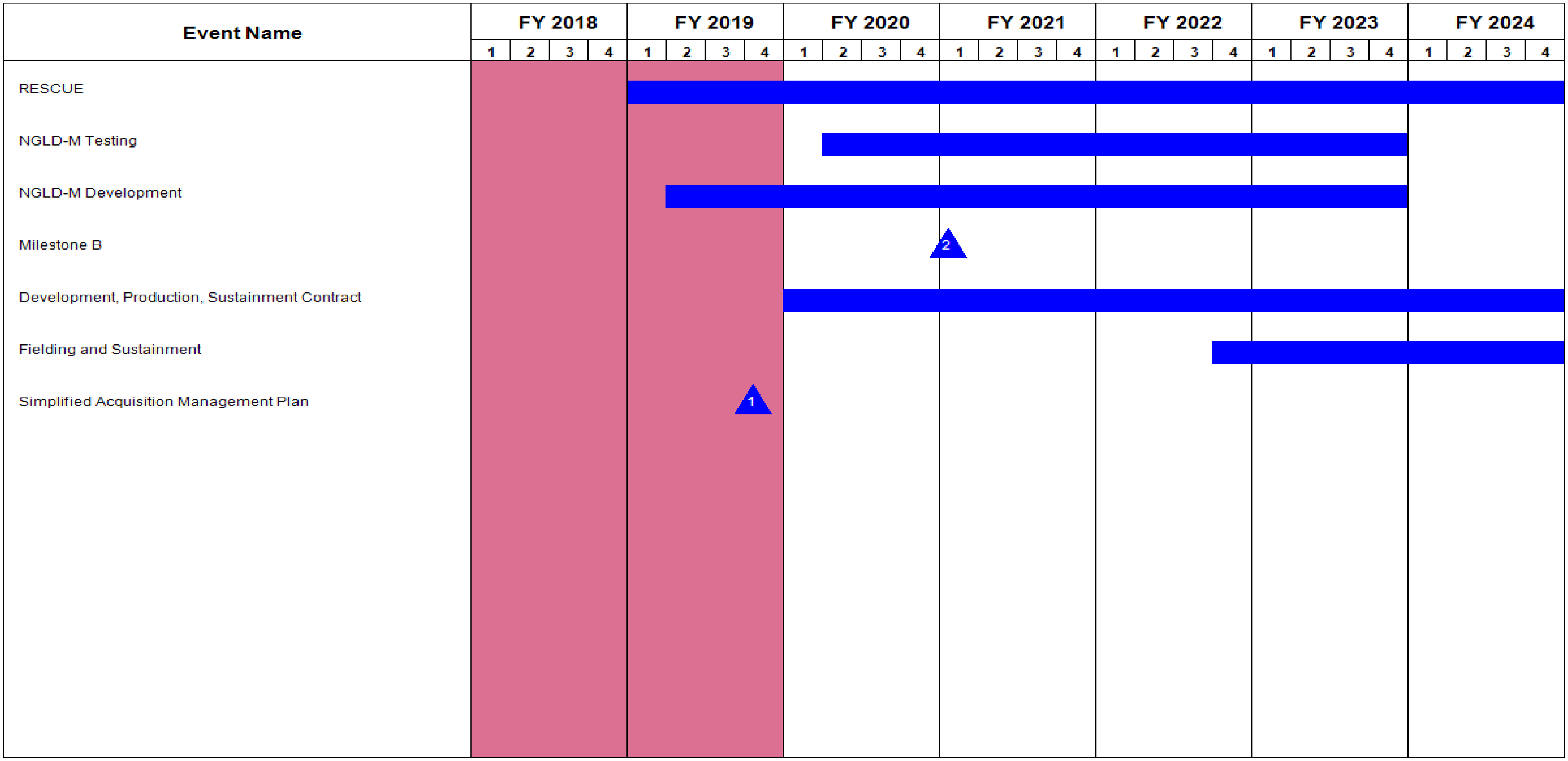

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 *I* 7	**R-1 Program Element (Number/Name)** PE 0303140A *I Information Systems Security Program*	**Project (Number/Name)** DV4 *I Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
RESCUE	1	2019	4	2024
NGLD-M Testing	2	2020	4	2023
NGLD-M Development	2	2019	4	2023
Milestone B	1	2021	1	2021
Development, Production, Sustainment Contract	1	2020	4	2024
Fielding and Sustainment	4	2022	4	2024
Simplified Acquisition Management Plan	4	2019	4	2019

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	26.055	7.943	7.630	-	7.630	7.812	7.900	10.187	8.048	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Project DV5, Crypto Modernization (Crypto Mod) supports the Army's Network Modernization Strategy Line of Effort (LOE) 1 Network Enablers Functions.

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. 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. The Army's Mission Command Network Modernization Implementation Plan states that LOE 1 to be a Unified Network which includes the attributes of being, "Protected, Resilient, Survivable" which Communications Security (COMSEC) is the Army's implementation of NSA protections to achieve LOE 1. Crypto Modernization is foundational to the Army's LOE 1: Network Enabling Functions.

This program supports using 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.

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 emerging Information Assurance (IA)/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 and the Army Modernization and Strategy Plan.

The Embedded Cryptographic Modernization Initiative (ECMI) is designed to investigate Courses Of Action, conduct a Material Solution Analysis, and execute upgrade activities to ensure all enduring Army communications and data equipment that employ embedded cryptographic hardware will utilize modern cryptographic algorithms and keys.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.820	0.625	0.746
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			

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
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 2019 Plans:*** Continue to test and evaluate any engineering changes to Full Rate Production (FRP) of VACM devices (the KYV-5M) 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 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 2019 to FY 2020 Increase/Decrease Statement:*** Additional Devices to be fielded 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 2019 Plans:*** 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, CHVP, CSfC Guidance, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 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 and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***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,	2.910	6.372	5.938

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army			**Date:** March 2019
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 2018**	**FY 2019**	**FY 2020**
CSfC Guidance, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 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 and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Reduction of Test and Evaluation on HAIPE devices.			
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 2019 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. This will facilitate the upgrade of the Army HAIPIES to include new cyber sensor functionality for the tactical cell. ***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 HAIPE extensions. This will facilitate the upgrade of the Army HAIPIES to include new cyber sensor functionality for the tactical cell.	1.748	0.946	0.946
Title: FY 2018 Recission	20.577	-	-
Accomplishments/Planned Programs Subtotals	26.055	7.943	7.630

C. Other Program Funding Summary ($ in Millions)

Line Item	**FY 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**Cost To Complete**	**Total Cost**
• 491: *Information Assurance Development*	9.787	10.159	8.368	-	8.368	8.017	7.604	7.645	5.600	Continuing	Continuing
• ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	48.914	20.745	0.000	-	0.000	-	-	-	-	0.000	69.659
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	47.536	26.350	72.457	-	72.457	36.113	26.399	30.776	39.721	Continuing	Continuing

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• B96006: *Embedded Cryptographic Modernization*	-	3.520	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.135	3.131	3.857	-	3.857	3.901	3.939	3.940	4.000	0.000	25.903

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by PL Net E, 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

D. Acquisition Strategy

The objective of this program is to integrate and validate 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 Cryptographic Systems 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. 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.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army			Date: March 2019
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)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
System Engineering	SS/LH	CECOM RDEC : APG, MD	3.687	1.896		1.809		1.809		-		1.809	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	4.880	1.761		1.750	Apr 2019	1.650	Apr 2019	-		1.650	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	2.336	1.996		2.034	Sep 2018	1.934	Sep 2018	-		1.934	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	3.324	1.982		1.959	Sep 2018	1.846	Sep 2018	-		1.846	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/CPFF	Envision : Aberdeen, Maryland	0.583	0.383		0.391	Jun 2018	0.391	Jun 2018	-		0.391	Continuing	Continuing	Continuing
Embedded Crypto Modernization Support	C/LH	TBD : TBD	19.733	18.037		-		-		-		-	Continuing	Continuing	Continuing
		Subtotal	34.543	26.055		7.943		7.630		-		7.630	Continuing	Continuing	N/A

	Prior Years	**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	34.543	26.055		7.943		7.630		-		7.630	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
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)*

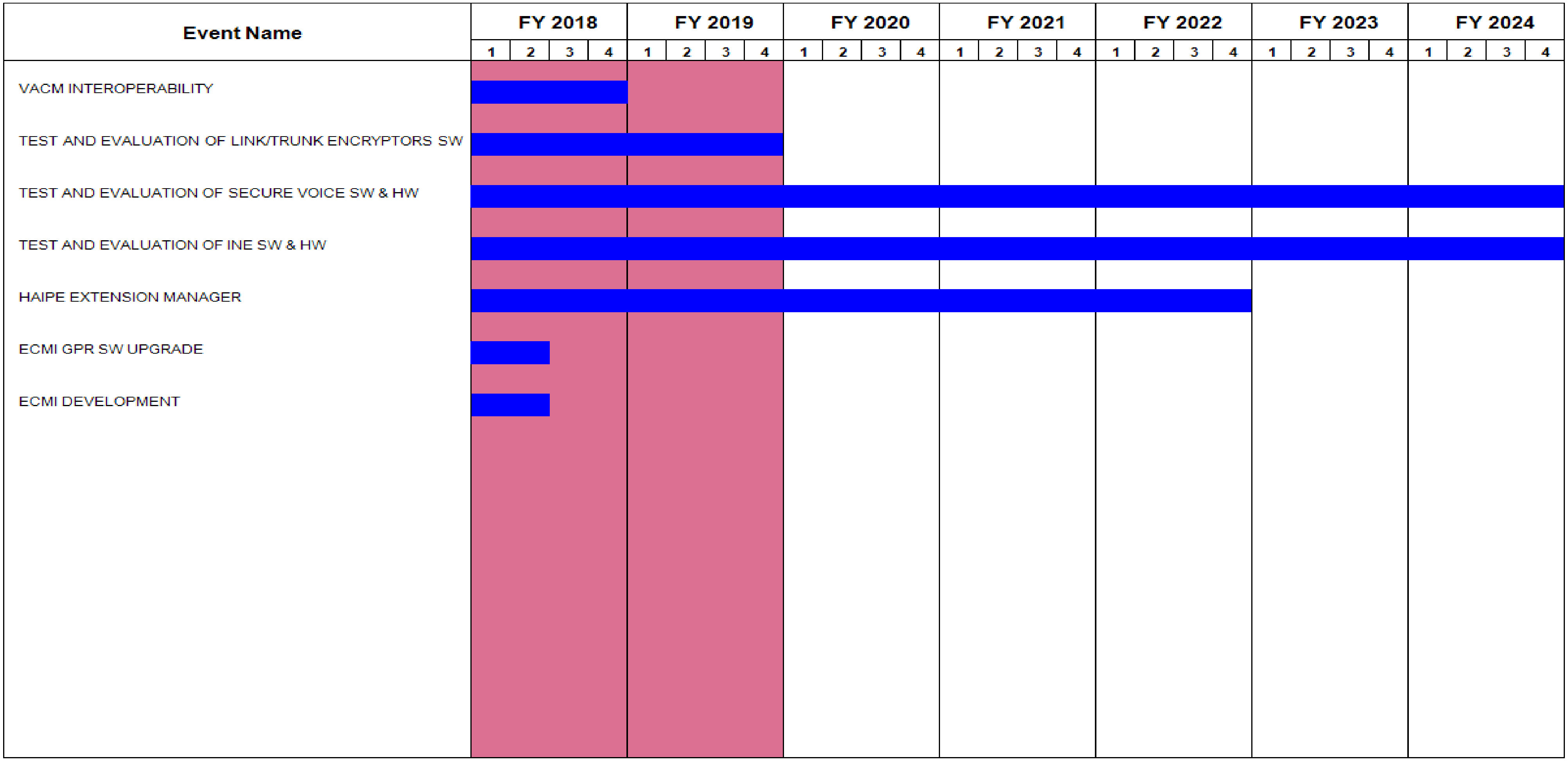

Exhibit R-4A, RDT&E Schedule Details: PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
VACM INTEROPERABILITY	1	2016	4	2018
TEST AND EVALUATION OF LINK/TRUNK ENCRYPTORS SW	1	2016	4	2019
TEST AND EVALUATION OF SECURE VOICE SW & HW	4	2013	4	2024
TEST AND EVALUATION OF INE SW & HW	1	2017	4	2024
HAIPE EXTENSION MANAGER	1	2017	4	2022
ECMI GPR SW UPGRADE	3	2016	2	2018
ECMI DEVELOPMENT	1	2017	2	2018

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	48.914	20.745	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	69.659
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 2018	FY 2019	FY 2020
Title: Embedded Cryptographic Modernization Initiative (ECMI) Development Contracts ***Description:*** ECMI Non Recurring Engineering (NRE) Contract Prep Work and Execution ***FY 2019 Plans:*** Support NRE development of ECMI efforts for vendor developmental and production contracts which supports NSA mandated Cease Key Date IAW CJCSI 6510.02E. This capability will ensure Army tactical radios operate with the latest cryptographic solutions. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Decrease of FY 2020 funding is due to change in Air-to-Ground radio acquisition strategy. The ARC-201D crypto modernization is no longer required.	0.761	20.745	-
Title: FY 2018 Rescission	48.153	-	-
Accomplishments/Planned Programs Subtotals	48.914	20.745	-

Exhibit R-2A, RDT&E Project Justification: PB 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	9.787	10.159	8.368	-	8.368	8.017	7.604	7.645	5.600	Continuing	Continuing
• DV5: *Crypto Modernization (Crypto Mod)*	26.055	7.943	7.630	-	7.630	7.812	7.900	10.187	8.048	Continuing	Continuing
• B96002: *CRYPTOGRAPHIC SYSTEMS (CRYPTO SYS)*	47.536	26.350	72.457	-	72.457	36.113	26.399	30.776	39.721	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	3.520	0.000	-	0.000	-	-	-	-	0.000	3.520
• BS9716: *NON PEO-SPARES*	3.135	3.131	3.857	-	3.857	3.901	3.939	3.940	4.000	0.000	25.903

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.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2020 Army		**Date:** March 2019
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)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
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)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
PM TR Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	2.985	4.968		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	4.409	27.720		20.745		-		-		-	0.000	52.874	N/A

Test and Evaluation ($ in Millions)				**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
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 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	4.409	48.914		20.745		-		-		-	0.000	74.068	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
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)*

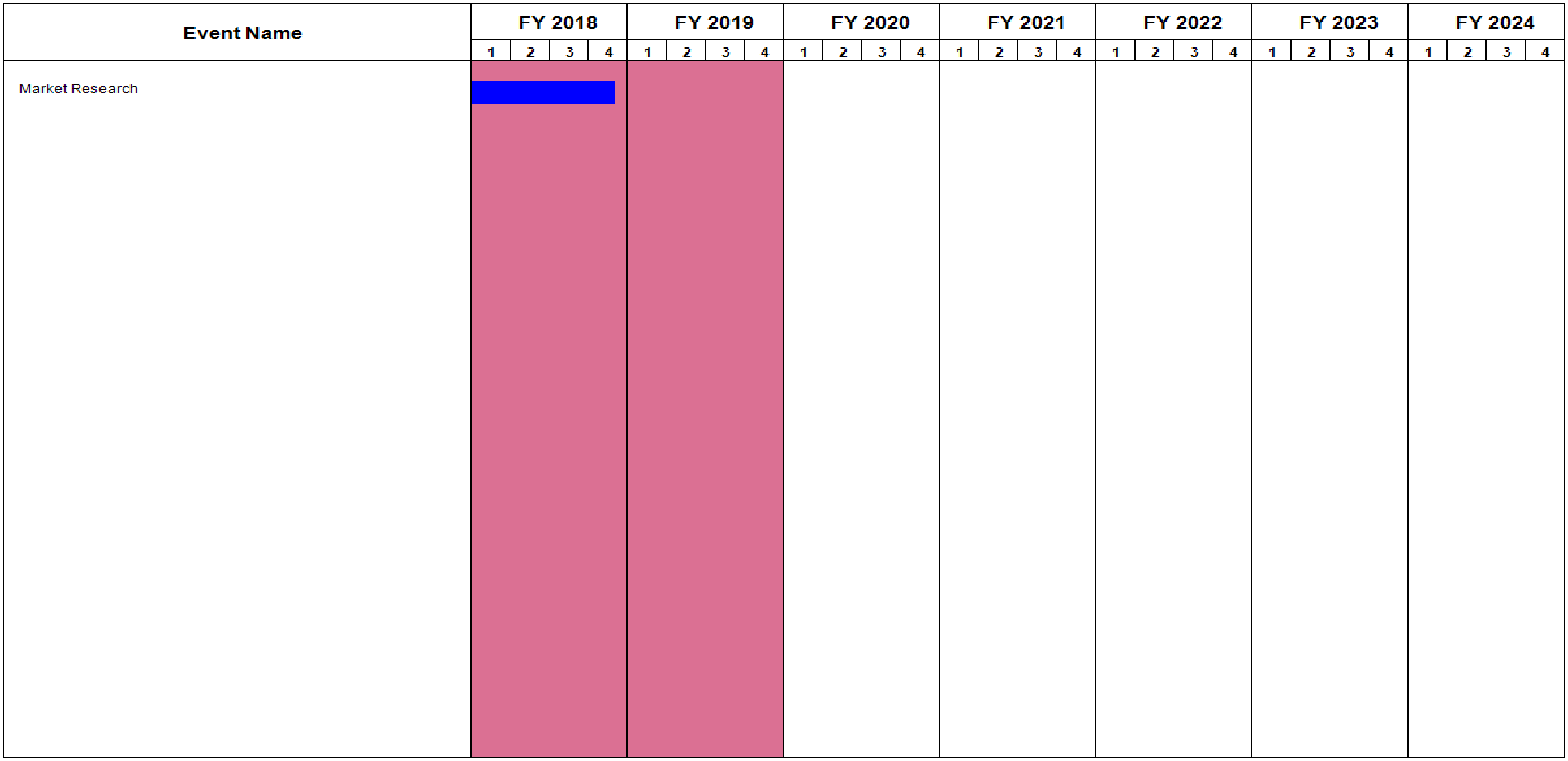

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army	**Date:** March 2019

Appropriation/Budget Activity	**R-1 Program Element (Number/Name)**	**Project (Number/Name)**
2040 **/** 7	PE 0303140A **/** *Information Systems Security Program*	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 2020 Army		**Date:** March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
FF8: *Unit Activity Monitoring (UAM)*	-	19.491	0.971	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	20.462
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 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. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
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). ***FY 2019 Plans:*** Continue Unit Activity Monitoring ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Program receives no funding in FY 2020	19.491	0.971	-
Accomplishments/Planned Programs Subtotals	19.491	0.971	-

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Army		**Date:** March 2019
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)*

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

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.

E. Performance Metrics

N/A

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 *I* 7	**R-1 Program Element (Number/Name)** PE 0303140A *I Information Systems Security Program*	**Project (Number/Name)** FF8 *I Unit Activity Monitoring (UAM)*

Product Development ($ in Millions)

				FY 2018		FY 2019		FY 2020 Base		FY 2020 OCO		FY 2020 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Software Engineering Development	C/TBD	TBD : TBD	-	19.491	Jun 2018	0.971	Jun 2019	-		-		-	0.000	20.462	Continuing
		Subtotal	-	19.491		0.971		-		-		-	0.000	20.462	N/A

	Prior Years	**FY 2018**		**FY 2019**		**FY 2020 Base**		**FY 2020 OCO**		**FY 2020 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	-	19.491		0.971		-		-		-	0.000	20.462	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2020 Army		**Date:** March 2019
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)*

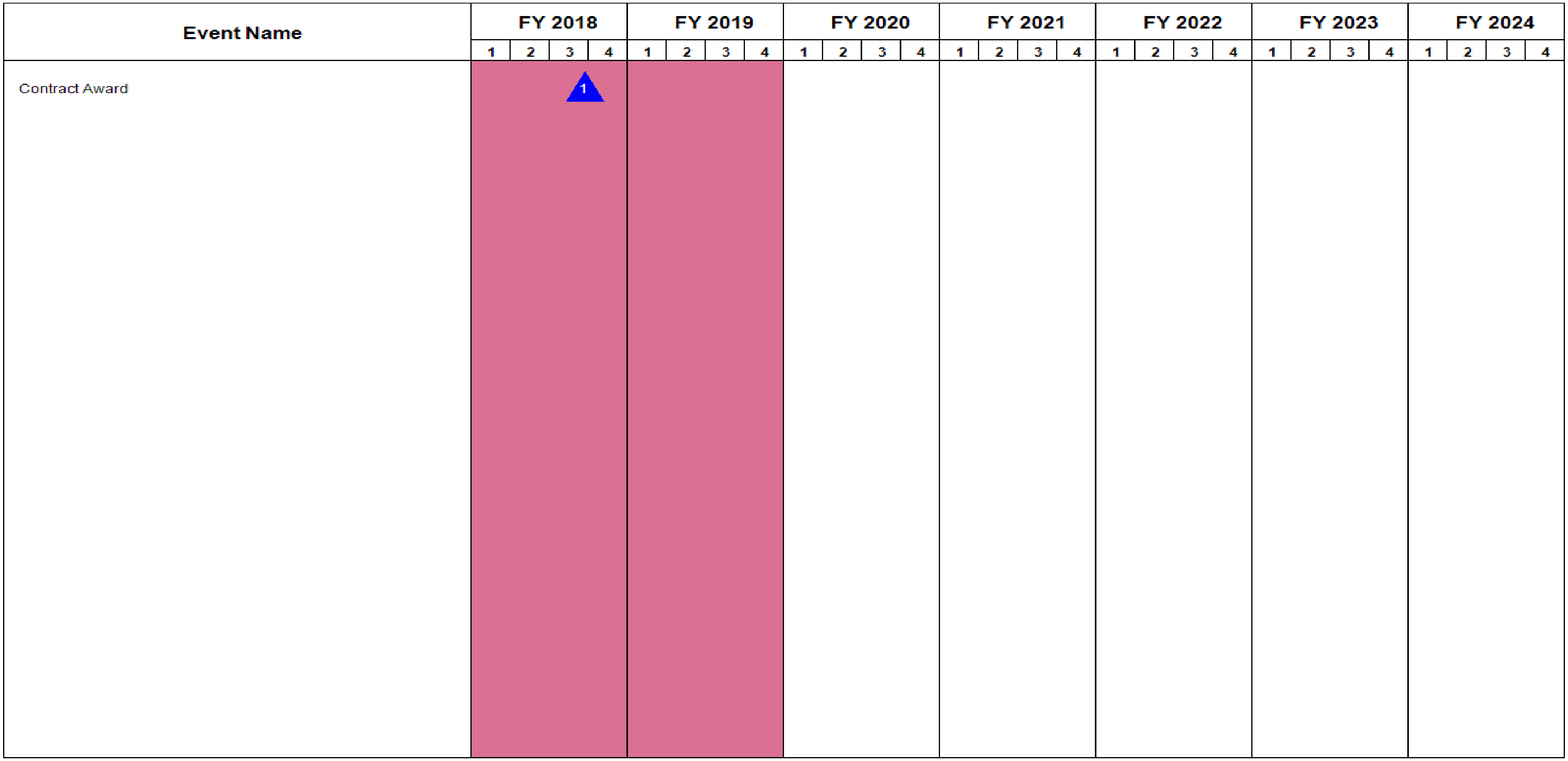

Exhibit R-4A, **RDT&E Schedule Details:** PB 2020 Army		**Date:** March 2019
Appropriation/Budget Activity 2040 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140A **/** *Information Systems Security Program*	**Project (Number/Name)** FF8 **/** *Unit Activity Monitoring (UAM)*

Schedule Details

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