Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Army											Date: February 2018	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140A *I Communications Security (COMSEC) Equipment*							
COST ($ in Millions)	**Prior Years**	**FY 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
Total Program Element	-	36.892	132.438	68.533	-	68.533	54.714	24.486	23.236	22.267	0.000	362.566
491: *Information Assurance Development*	-	7.145	10.194	10.172	-	10.172	10.668	11.317	10.104	10.245	0.000	69.845
DV4: *Key Management Infrastructure (KMI)*	-	4.518	4.696	2.702	-	2.702	3.265	3.543	3.415	0.000	0.000	22.139
DV5: *Crypto Modernization (Crypto Mod)*	-	20.820	27.047	25.831	-	25.831	24.824	8.580	8.646	10.936	0.000	126.684
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	4.409	88.949	28.857	-	28.857	14.974	0.000	0.000	0.000	0.000	137.189
FF8: *Unit Activity Monitoring (UAM)*	-	0.000	1.552	0.971	-	0.971	0.983	1.046	1.071	1.086	0.000	6.709

A. Mission Description and Budget Item Justification

Information Assurance 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 and the Army Modernization and Strategy Plan.

Information Assurance Development funding implements and establishes functional and technical boundaries of cryptographic, key management and Information Assurance (IA) capabilities in coordination with 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 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 Department of Defense (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.

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.

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 Family of fill devices. The NSA Key Management Infrastructure (KMI) Program replaced NSA EKMS program. AKMI has replaced Army Key Management System. The transition from AKMS to AKMI started in FY12. The AKMS System of Systems (SoS) systems components are the Local COMSEC Management Software (LCMS), Automated Communications Engineering Software (ACES) and Simple Key Loader (SKL).

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 specified 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 Strategic Planning Guidance and the Army Modernization and Strategy Plan.

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.

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

Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Army	Date: February 2018
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140A *I Communications Security (COMSEC) Equipment*

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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Previous President's Budget	38.280	132.438	90.008	-	90.008
Current President's Budget	36.892	132.438	68.533	-	68.533
Total Adjustments	-1.388	0.000	-21.475	-	-21.475
• Congressional General Reductions	-0.017	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-1.371	-			
• Adjustments to Budget Years	-	-	-21.475	-	-21.475

Change Summary Explanation

FY 2017 decrease of $1.388 million for FFRDC and SBIR/STTR adjustments.

FY 2019 decrease of $21.475 million based on requirement adjustments.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army											Date: February 2018	
Appropriation/Budget Activity 2040 / 7					R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*				Project (Number/Name) 491 / *Information Assurance Development*			
COST ($ in Millions)	**Prior Years**	**FY 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
491: *Information Assurance Development*	-	7.145	10.194	10.172	-	10.172	10.668	11.317	10.104	10.245	0.000	69.845
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

This program supports the implementation of 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; integrating these mechanisms into specified systems in support of securing the Army Tactical and Enterprise Network.

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, camps and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization Strategy Plan.

Implement, establish functional and technical boundaries of cryptographic, key management and Information Assurance (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 concept 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 evaluation, standards testing, and CS System of System Network Vulnerability Assessments (SoS NVA) Army Capability Sets for CS/COMSEC capabilities that provide protections for the tactical and fixed infrastructure post, camps, and station 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

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** 491 / *Information Assurance Development*

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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
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) ***FY 2018 Plans:*** As the Army implements new network technology, Secure Voice (SV) and In-line Network Encryption (INE) devices must continue to be identified and tested for effectiveness and suitability. Key areas of investigation include cyber security, interoperability, and standards compliance. (PL Net E) ***FY 2018 to FY 2019 Increase/Decrease Statement:*** No funding allocated in FY19 and outyears	1.170	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 2018 Plans:*** Oversee execution of the Army's COMSEC Modernization initiative by identifying and developing new security baseline for implementation of Army CM and KM initiatives. Assess, review and validate Army operational needs. Test and evaluate CM and KM technologies to determine the maturity and viability for Army use to protect and strengthen the Network posture. Identify fundamental building blocks for IA solutions, perform risk	5.975	8.728	10.172	-	10.172

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
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 and Joint Staff to define new ACC standards (security and interoperability) for the tactical and operational environment. Provide continuous 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 for protecting National Security Systems and National Information. Develop strategies and policies that leverage emerging cryptographic and key management tools and services. (CIO/G6) ***FY 2019 Base Plans:*** Oversee executions of the Army's COMSEC Modernization initiatives. Identify and develop new security baseline for Army implementation in the areas of CM and KM. Develop end-to-end, tactical-to-strategic COMSEC standardization to meet Army?s operational needs and requirements. Test and evaluate 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 and Joint Staff to continue to define the second phase of ACC standards (security and interoperability) for the tactical and operational environment. 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. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Economic adjustment.					
Accomplishments/Planned Programs Subtotals	7.145	10.194	10.172	-	10.172

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• DV5: *Crypto Modernization*	20.820	27.047	25.831	-	25.831	24.824	8.580	8.646	10.936	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) 491 / *Information Assurance Development*	

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• ET9: *Embedded Crypto Modernization*	4.409	88.949	28.857	-	28.857	14.974	-	-	-	0.000	137.189
• B96002: *Cryptographic Systems*	66.692	49.441	49.107	0.003	49.110	104.421	106.898	103.106	109.001	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	3.014	-	3.520	-	3.520	97.959	157.904	48.382	5.013	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	2.545	3.135	3.131	-	3.131	4.857	4.901	4.939	4.940	Continuing	Continuing

Remarks

Line Item and Title:
DV5 - Crypto Modernization - RDTE
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 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 10; ICD, approved by JROC, 25 Mar 11; AAO; approved by G3, 15 Dec 11 and revised and approved, 19 Jun 15.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) 491 / *Information Assurance Development*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PL Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	79.147	1.170		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	120.852	1.170		1.466		-		-		-	0.000	123.488	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 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	5.124	1.309		2.196		2.496		-		2.496	Continuing	Continuing	-
System Engineering (CIO/G-6)	SS/LH	CECOM RDEC : APG, MD	3.771	1.086		1.496		2.196		-		2.196	Continuing	Continuing	-
Engineering Support (CIO/G-6)	C/CPFF	Booz Allen Hamilton : APG, MD	6.188	1.261		1.737		1.897		-		1.897	Continuing	Continuing	-
Engineering Support (CIO/G-6)	C/FFP	AASKI : Edgewood, MD	2.111	1.316		1.813		2.372		-		2.372	Continuing	Continuing	-
Service (CIO-G-6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	4.969	1.003		1.486		1.211		-		1.211	Continuing	Continuing	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) 491 / *Information Assurance Development*	

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	23.761	5.975		8.728		10.172		-		10.172	Continuing	Continuing	N/A

Remarks

Not Applicable

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	144.613	7.145		10.194		10.172		-		10.172	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** 491 / *Information Assurance Development*

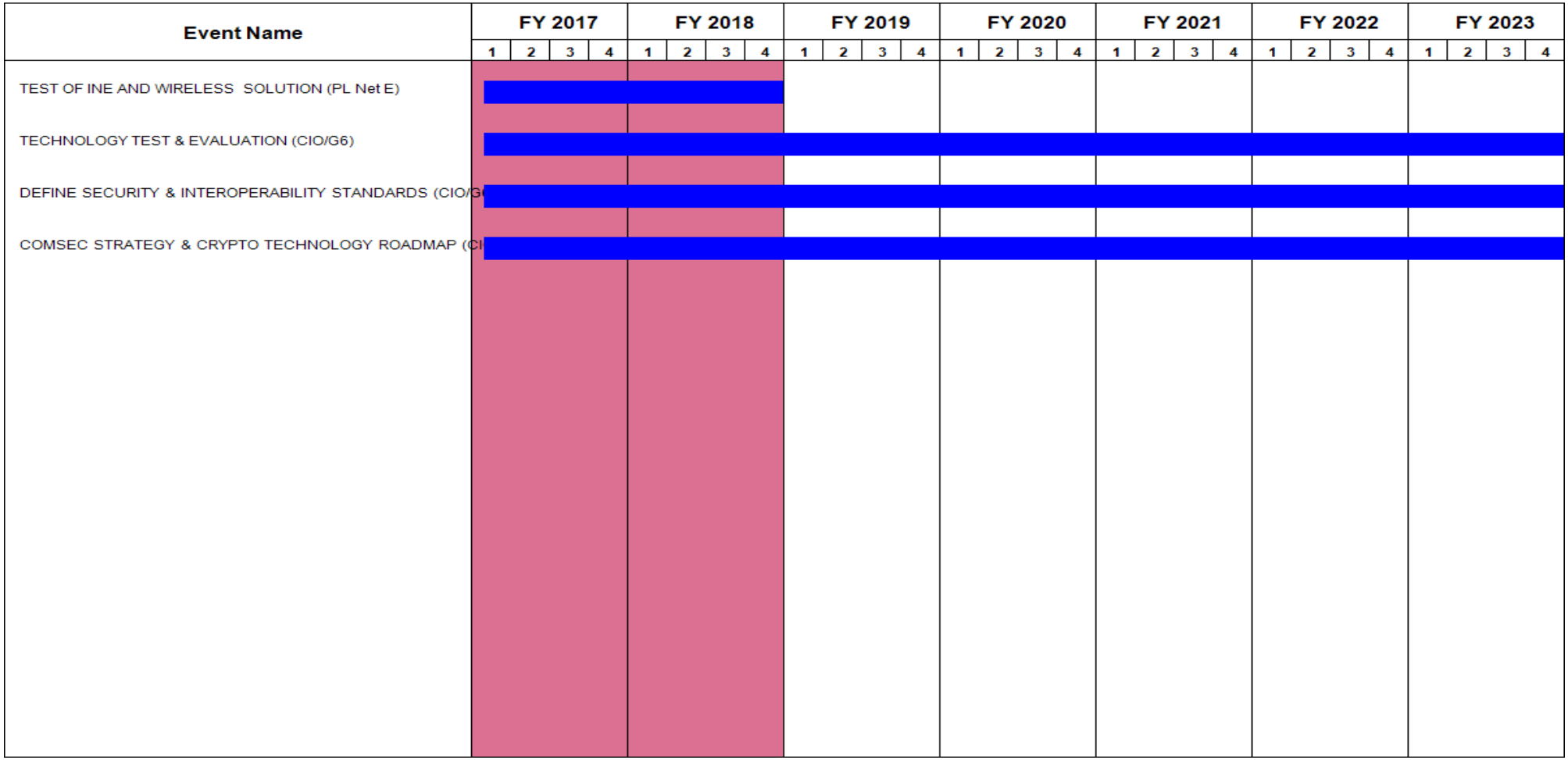

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** 491 / *Information Assurance Development*

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 2019 Army											Date: February 2018	
Appropriation/Budget Activity 2040 / 7					R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*				Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*			
COST ($ in Millions)	**Prior Years**	**FY 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
DV4: *Key Management Infrastructure (KMI)*	-	4.518	4.696	2.702	-	2.702	3.265	3.543	3.415	0.000	0.000	22.139
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Key Management Infrastructure (KMI) funding line DV4 was established in FY2014. Army Key Management System (AKMS) funding line 501 realigned to KMI funding line DV4 in FY2017. AKMI supports infrastructure requirements in support of Key Management.

A. Mission Description and Budget Item Justification

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 and Medium. 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 Crypto 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.

The NGLD Medium is reliant on the Reprogrammable Single Chip Universal Encryptor (RESCUE), a new KMI compliant cryptographic engine that is currently being developed. The KOV-21 card currently used in Army Simple Key Loader (SKL) fill devices has hardware obsolescence issues and does not support OTNK. Redesign and developmental efforts using modern and readily available components for use in the Army's SKL devices have been initiated under the RESCUE program. The current KOV-21 card is referred to as the KOV-21 Replacement and is an extension of the RESCUE program as a technology insertion. The follow-on RESCUE technology development will start in FY2018.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: Key Management Infrastructure (KMI) Awareness (RESCUE / KOV-21 Replacement Effort)	4.518	4.696	2.702	-	2.702
Description: KMI Awareness initiative creates a secure, highly automated interface in providing future Over the Network Keying (OTNK) capability to legacy End Crypto Units (ECU)s. This initiative will allow ECUs to receive, authenticate, and decrypt OTNK messages and increases WarFighter survivability by minimizing the need for Soldiers to travel to obtain keys. The KOV 21 card, previously in production through NSA for use in the Simple Key Loader (SKL) and the Secure DTD 2000 System (SDS), is nearing the end of life due to unavailability of parts. Redesigning and developmental efforts using modern and readily available components for use in the Army's SKL and Next Generation Load Devices (NGLDs) are currently underway. The redesign of the current KOV 21 card is referred to as the KOV 21 Replacement and is an extension of the KOV 21 card as a technology insertion. The KOV 21 Replacement will also address requirements codified in the NGLD CPD and the AKMI CPD that were technologically unachievable with the KOV 21 card. ***FY 2018 Plans:*** The RESCUE technology development will complete in FY2018. RESCUE development will provide the ability to upgrade legacy ECUs, enabling a KMI aware fully developed PDE-enabled ECU fleet. The KOV-21 Replacement effort lays the foundation for AKMI capabilities that can be inserted into the SKL to make it an NGLD Medium. ***FY 2019 Base Plans:*** The follow-on RESCUE technology will continue in FY2019. ***FY 2018 to FY 2019 Increase/Decrease Statement:*** The follow-on RESCUE technology will continue in FY2019.					
Accomplishments/Planned Programs Subtotals	4.518	4.696	2.702	-	2.702

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	63.578	58.363	35.710	-	35.710	97.061	99.098	89.919	115.498	Continuing	Continuing
• 432140: *ISSP (TSEC-AKMS)*	7.966	8.319	8.682	-	8.682	3.950	4.048	4.124	4.194	Continuing	Continuing

Remarks

Line Item & Title:

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
B96004: Key Management Infrastructure (OPA2)											
432140: 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.

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 fill devices and Tier 3 component of the AKMI Program. The NGLD Capability Production Document (CPD) was signed 4QFY13. The NGLD CPD calls for a family of 2 devices (small and medium) 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 Army will gain the NGLD Medium capability through the SKL v3.1 in combination with a new KMI compliant cryptographic engine, the RESCUE, the first iteration of the RESCUE being the KOV-21 Replacement. The redesign of the current SKL cryptographic engine, the KOV-21 card, is required due to parts obsolescence and inability to be KMI Aware. The KOV-21 Replacement is an extension of the RESCUE program as a technology insertion into the SKL v3.1 which in turn meets the NGLD Medium CPD requirements. The NGLD Medium will be available in FY19. The follow-on RESCUE technology development will start in FY2019.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
KMI Awareness (RESCUE / KOV-21 Replacement Effort)	C/CPFF	Dynamics Research Corporation/Engility : APG, MD	4.011	4.518	Jul 2017	4.696	Jul 2018	-		-		-	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CERDEC, S&TCD : APG, MD	1.451	-		-		-		-		-	0.000	1.451	-
RESCUE Embedment	C/TBD	CERDEC STCD : APG, MD	-	-		-		2.702	Dec 2018	-		2.702	Continuing	Continuing	Continuing
		Subtotal	5.462	4.518		4.696		2.702		-		2.702	Continuing	Continuing	N/A

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	5.462	4.518		4.696		2.702		-		2.702	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

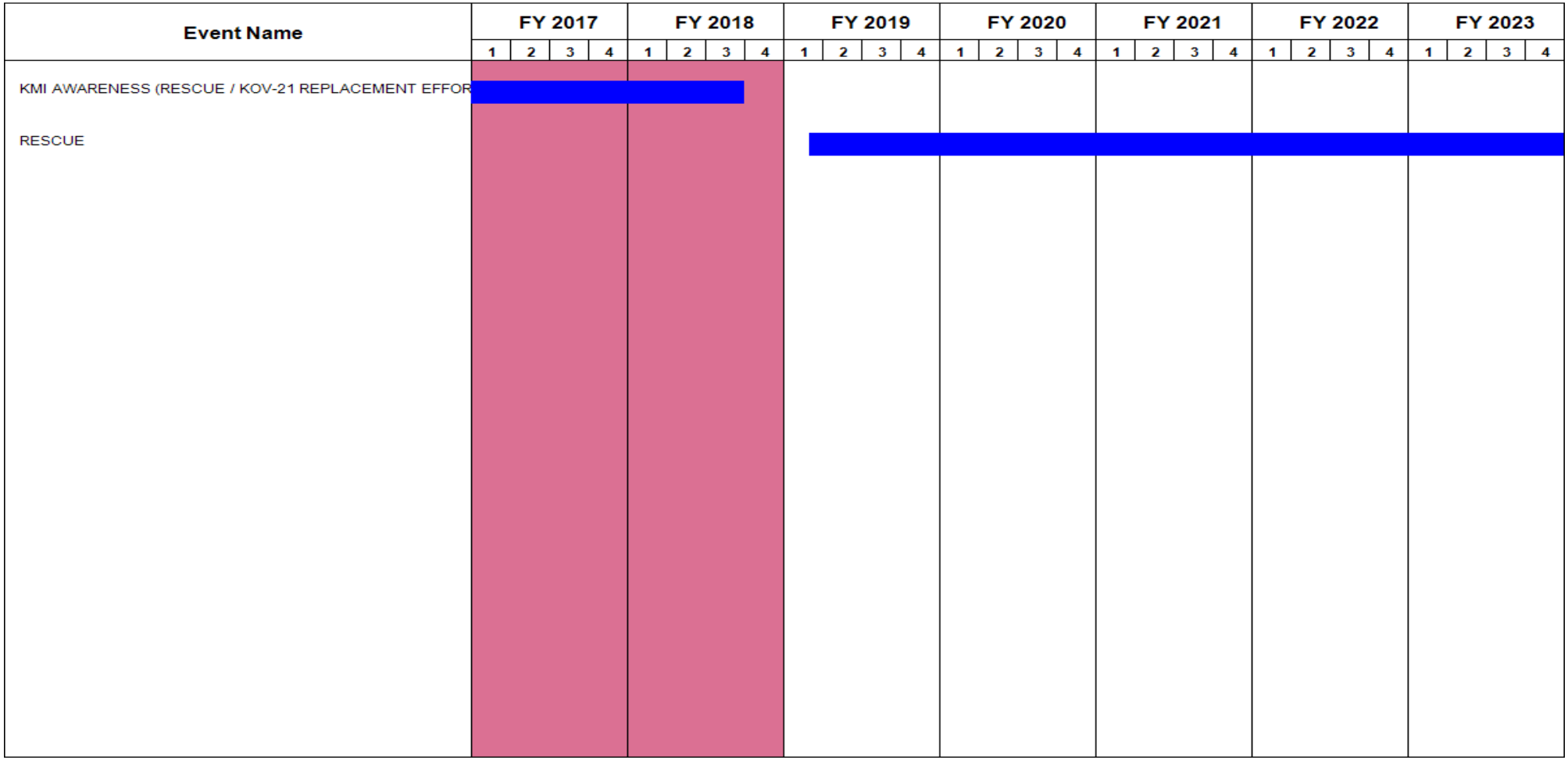

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
KMI AWARENESS (RESCUE / KOV-21 REPLACEMENT EFFORT)	4	2015	3	2018
RESCUE	1	2019	4	2023

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

COST ($ in Millions)	Prior Years	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	20.820	27.047	25.831	-	25.831	24.824	8.580	8.646	10.936	0.000	126.684
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

DV5 - The Crypto Modernization line was established in Sept 2012.

A. Mission Description and Budget Item Justification

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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.919	0.600	1.059	-	1.059
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-100 and CV- 3591 / KYV-5. In order to ensure the confidentiality, integrity and availability of classified communications, the cryptographic modules must be tested for interoperability and form fit to ensure a successful fielding. Each software release will require testing to insure comparability and interoperability.					
FY 2018 Plans:					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
The program will continue to test and evaluate 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 begin fielding, performing site surveys and installing at both CONUS and OCONUS locations. ***FY 2019 Base 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 2018 to FY 2019 Increase/Decrease Statement:*** Additional test and evaluation required for FRP VACM Devices.					
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 2018 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 2019 Base 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	4.303	5.450	5.938	-	5.938

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
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 2018 to FY 2019 Increase/Decrease Statement:*** Increase in CTR support.					
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 2018 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 HAIPEs to include new cyber-sensor functionality for the tactical cyber cell. ***FY 2019 Base 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 2018 to FY 2019 Increase/Decrease Statement:*** Decrease in Matrix and SETA manpower costs.	1.095	1.748	0.946	-	0.946
Title: Embedded Cryptographic Modernization Initiative (ECMI) ***Description:*** The ECMI is an upgrade activity that will ensure enduring Army radios remain secure by operating with modern cryptographic algorithms and keys. Funding secured in DV5 line to support ECMI Non Recurring Engineering (NRE) efforts to comply with cease key dates mandated by CJCSI 6510. ***FY 2018 Plans:*** Continue execution of NRE efforts to develop, design, test/evaluate, and certify cryptographic hardware and software embedded in tactical radios to ensure these radios remain secure. System engineering activities	14.503	19.249	17.888	-	17.888

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
including detailed requirements decomposition, functional allocation, design of modern reprogrammable cryptographic modules, and detailed hardware design and software coding.					
FY 2019 Base Plans: Continue execution of NRE efforts to develop, design, test/evaluate, and certify cryptographic hardware and software embedded in tactical radios to ensure these radios remain secure. System engineering activities including detailed requirements decomposition, functional allocation, design of modern reprogrammable cryptographic modules, and detailed hardware design and software coding.					
FY 2018 to FY 2019 Increase/Decrease Statement: ECMI R&D efforts will be entering the final stages in FY19 and beyond. Future efforts will be funded using OPA dollars.					
Accomplishments/Planned Programs Subtotals	20.820	27.047	25.831	-	25.831

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	7.145	10.194	10.172	-	10.172	10.668	11.317	10.104	10.245	Continuing	Continuing
• ET9: *Embedded Crypto Modernization*	4.409	88.949	28.857	-	28.857	14.974	-	-	-	0.000	137.189
• B96002: *Cryptographic Systems*	66.692	49.441	49.107	0.003	49.110	104.421	106.898	103.106	109.001	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	3.014	-	3.520	-	3.520	97.959	157.904	48.382	5.013	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	2.545	3.135	3.131	-	3.131	4.857	4.901	4.939	4.940	Continuing	Continuing

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

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
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 10; ICD, approved by JROC, 25 Mar 11; AAO; approved by G3, 15 Dec 11 and revised and approved, 19 Jun 15.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CECOM RDEC : APG, MD	2.237	1.450		1.796		1.809		-		1.809	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	3.583	1.297	Apr 2017	1.641		1.750	Apr 2019	-		1.750	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.695	1.641	Sep 2016	1.996		2.034	Sep 2018	-		2.034	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	1.596	1.728	Sep 2016	1.982		1.959	Sep 2018	-		1.959	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/CPFF	Envision : Aberdeen, Maryland	0.382	0.201	Jun 2016	0.383		0.391	Jun 2018	-		0.391	Continuing	Continuing	Continuing
Embedded Crypto Modernization Support	C/LH	TBD : TBD	5.230	14.503		19.249		17.888		-		17.888	Continuing	Continuing	Continuing
		Subtotal	13.723	20.820		27.047		25.831		-		25.831	Continuing	Continuing	N/A

	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	13.723	20.820		27.047		25.831		-		25.831	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

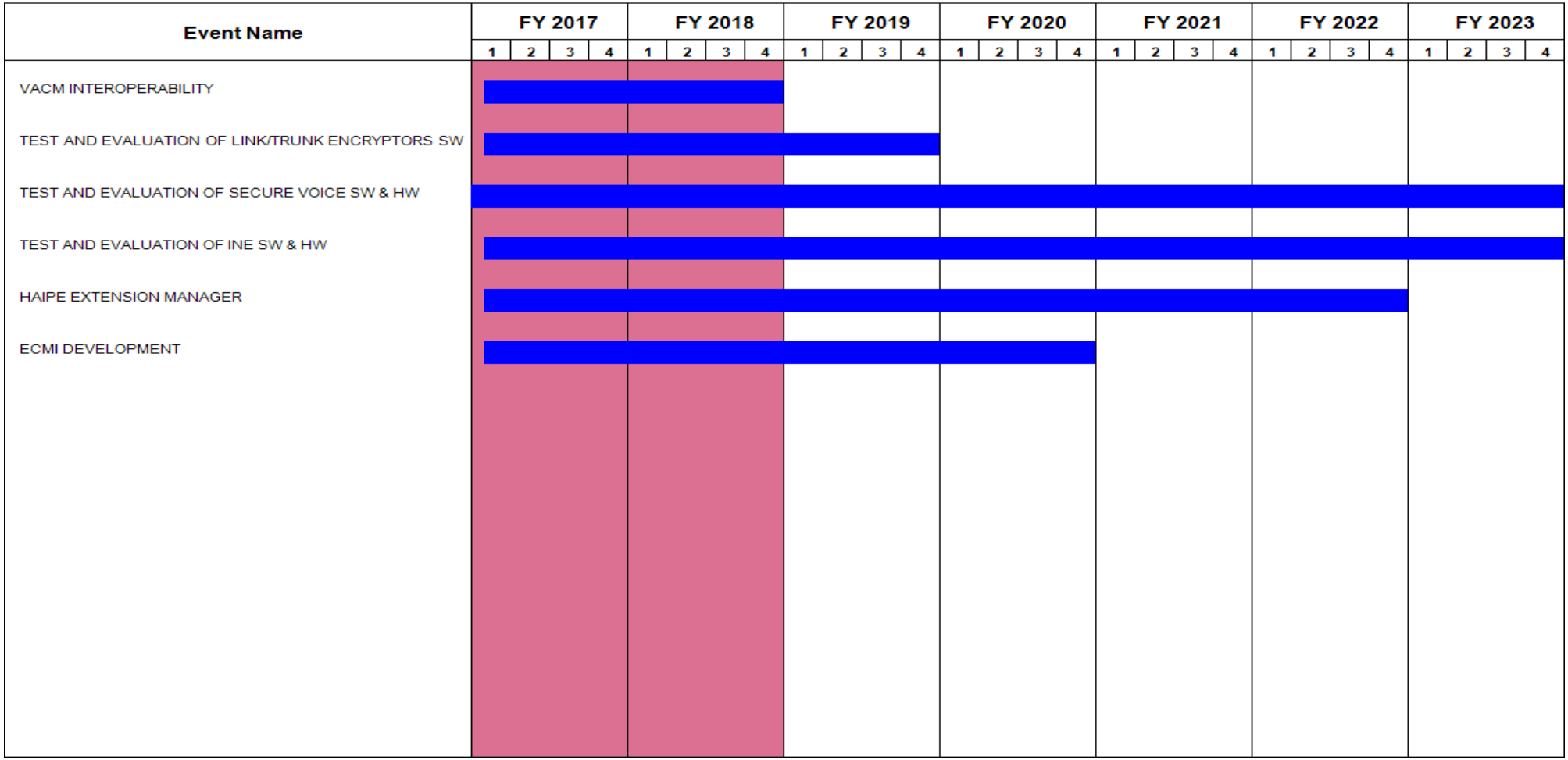

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

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	2023
TEST AND EVALUATION OF INE SW & HW	1	2017	4	2023
HAIPE EXTENSION MANAGER	1	2017	4	2022
ECMI DEVELOPMENT	1	2017	4	2020

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*	

COST ($ in Millions)	Prior Years	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	4.409	88.949	28.857	-	28.857	14.974	0.000	0.000	0.000	0.000	137.189
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

ET9 - The Embedded Crypto Modernization Initiative (ECMI) line was established in July 2015

A. Mission Description and Budget Item Justification

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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: Embedded Cryptographic Modernization Initiative (ECMI) Development Contracts	4.409	88.949	28.857	-	28.857
Description: ECMI Non Recurring Engineering (NRE) Contract Prep Work and Execution ***FY 2018 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 Base 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 2018 to FY 2019 Increase/Decrease Statement:*** Funding in FY19 was realigned by HQDA in order to fund other priority requirements.					
Accomplishments/Planned Programs Subtotals	4.409	88.949	28.857	-	28.857

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	7.145	10.194	10.172	-	10.172	10.668	11.317	10.104	10.245	Continuing	Continuing
• DV5: *Crypto Modernization*	20.820	27.047	25.831	-	25.831	24.824	8.580	8.646	10.936	Continuing	Continuing
• B96002: *Cryptographic Systems*	66.692	49.441	49.107	0.003	49.110	104.421	106.898	103.106	109.001	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	3.014	-	3.520	-	3.520	97.959	157.904	48.382	5.013	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	2.545	3.135	3.131	-	3.131	4.857	4.901	4.939	4.940	Continuing	Continuing

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 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PL NET E Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	-	2.663		4.968		1.612		-		1.612	Continuing	Continuing	Continuing
PM TR Program Mgmt Personnel	C/CPFF	BAH : Aberdeen, MD	-	1.424		-		-		-		-	Continuing	Continuing	Continuing
PM TR Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	-	0.322		-		-		-		-	Continuing	Continuing	Continuing
ECMI Development Contracts	C/CPFF	TBD : TBD	-	-		83.981		27.245		-		27.245	Continuing	Continuing	Continuing
		Subtotal	-	4.409		88.949		28.857		-		28.857	Continuing	Continuing	N/A

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	4.409		88.949		28.857		-		28.857	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

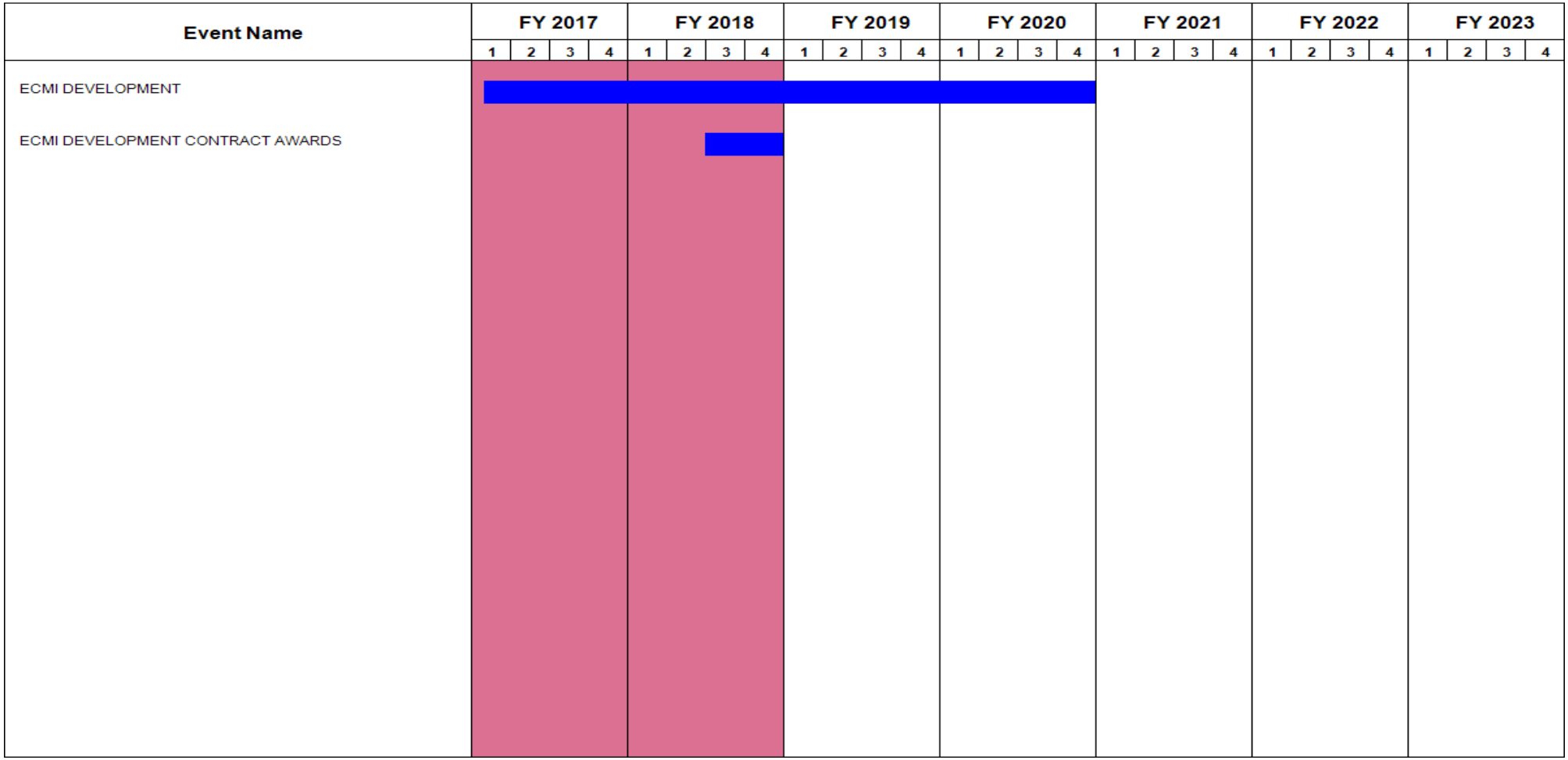

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
ECMI DEVELOPMENT	1	2017	4	2020
ECMI DEVELOPMENT CONTRACT AWARDS	3	2018	4	2018

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) FF8 / *Unit Activity Monitoring (UAM)*	

COST ($ in Millions)	Prior Years	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
FF8: *Unit Activity Monitoring (UAM)*	-	0.000	1.552	0.971	-	0.971	0.983	1.046	1.071	1.086	0.000	6.709
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: Unit Activity Monitoring	-	1.552	0.971	-	0.971
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 2018 Plans:*** Unit Activity Monitoring ***FY 2019 Base Plans:*** Unit Activity Monitoring ***FY 2018 to FY 2019 Increase/Decrease Statement:***					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Requirement decrease from FY18 to FY19.					
Accomplishments/Planned Programs Subtotals	-	1.552	0.971	-	0.971

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 2019 Army			Date: February 2018
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Communications Security (COMSEC) Equipment*	Project (Number/Name) FF8 / *Unit Activity Monitoring (UAM)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Engineering Development	C/TBD	TBD : TBD	-	-		1.552	Jun 2018	0.971	Jun 2019	-		0.971	0.000	2.523	Continuing
		Subtotal	-	-		1.552		0.971		-		0.971	0.000	2.523	N/A

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	-		1.552		0.971		-		0.971	0.000	2.523	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

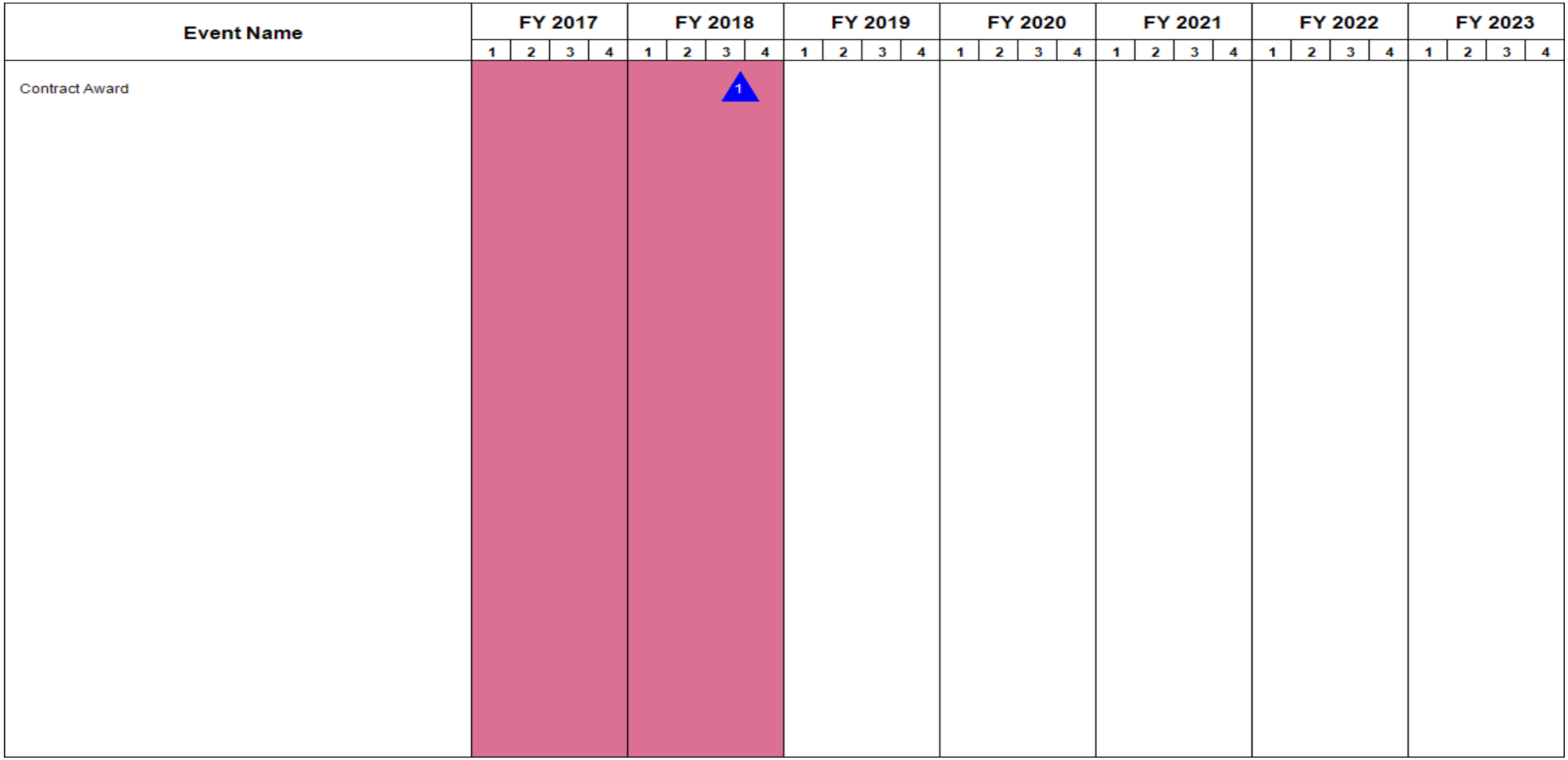

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Army		Date: February 2018
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Communications Security (COMSEC) Equipment*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

Schedule Details

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