Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Army											Date: February 2016	
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 2015**	**FY 2016**	**FY 2017 Base**	**FY 2017 OCO**	**FY 2017 Total**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**Cost To Complete**	**Total Cost**
Total Program Element	-	13.627	31.154	38.280	-	38.280	70.554	36.106	32.807	33.653	Continuing	Continuing
491: *Information Assurance Development*	-	6.922	18.009	7.431	-	7.431	10.092	8.783	9.228	9.814	Continuing	Continuing
501: *Army Key Mgt System*	-	1.138	1.927	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	3.065
DV4: *Key Management Infrastructure (KMI)*	-	2.081	2.009	4.699	-	4.699	4.782	3.333	0.000	3.395	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	3.486	9.209	21.565	-	21.565	28.424	23.990	23.579	20.444	Continuing	Continuing
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	0.000	0.000	4.585	-	4.585	27.256	0.000	0.000	0.000	0.000	31.841

A. Mission Description and Budget Item Justification

Information Assurance Development supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies into 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 National Network Enterprise in as transparent a manner as possible. 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 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.

Information Assurance Development funding Implements and establishes functional and technical boundaries of cryptographic, key management and IA capabilities In Coordination with (ICW) the National Security Agency (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 Cryptographic Modernization strategy to identify, standardize, and govern the insertion of IA 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 IAW the Army Network Campaign Plan. This will be accomplished by interoperability evaluation, standards testing, and IA System of System Network Vulnerability Assessments (IA SoS NVA) of Army Capability Sets for IA/COMSEC capabilities that provide protections for 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 System (AKMS) is the Army's implementation of the National Security Agency's (NSA) Electronic Key Management System (EKMS) program automating the functions of Communications Security (COMSEC) electronic key management, control, planning, and distribution. AKMS 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 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 NSA EKMS program is being replaced by the NSA Key Management Infrastructure (KMI) Program. The transition of the legacy EKMS LCMS to the modern KMI Management Client Nodes (MGC)s began in FY12 and must be completed by the EKMS Tier 2 sunset date of December 2017. AKMS supports the transition to Army Key Management Infrastructure (AKMI).

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 Crypto Modernization Initiatives 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), 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 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 Cryptographic Modernization Initiatives (CMI).

The Crypto Modernization 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 National Network Enterprise in as transparent a manner as possible. 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Army	Date: February 2016
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*

Embedded Cryptographic Modernization Initiative (ECMI) is an upgrade activity that will ensure enduring Army radios remain secure by operating with modern crypto keys. Tactical radios using embedded cryptographic systems will no longer be able to communicate securely after Crypto Keys expire due to 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 modernize their cryptographic capabilities by implementing the modern algorithms. If cease key dates are not met, Army will be forced to communicate at risk.

B. Program Change Summary ($ in Millions)	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Previous President's Budget	14.167	31.154	25.687	-	25.687
Current President's Budget	13.627	31.154	38.280	-	38.280
Total Adjustments	-0.540	0.000	12.593	-	12.593
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Years	-0.320	-	-3.567	-	-3.567
• DV4&DV5	-0.220	-	11.575	-	11.575
• ET9	-	-	4.585	-	4.585

Change Summary Explanation

In FY17 the following net adjustments were made:
Information Assurance Devleopment (491): Reduction of $.275M
Army Key Management (501): Reduction of $0.045M
Key Management Infrastructure (DV4): Increase of $2.317M
Crypto Modernization (DV5): Increase of $9.258M for government purpose rights software upgrades and development contracts.
Embedded Crypto Modernization (ET9): Funding line was added in the amount of $4.585 million for embedded crypto modernization in Army radios.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	6.922	18.009	7.431	-	7.431	10.092	8.783	9.228	9.814	Continuing	Continuing
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 into the Army by providing COMSEC system capabilities through encryption, trusted software, or standard operating procedures; and integrating these mechanisms into specified systems in support of securing the National Network Enterprise in as transparent a manner as possible.

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 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.

Implement and establish functional and technical boundaries of cryptographic, key management and IA capabilities In Coordination with (ICW) the National Security Agency (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 Cryptographic Modernization strategy to identify, standardize, and govern the insertion of IA 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 IAW the Army Network Campaign Plan. This will be accomplished by interoperability evaluation, standards testing, and IA System of System Network Vulnerability Assessments (IA SoS NVA) of Army Capability Sets for IA/COMSEC capabilities that provide protections for 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 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 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**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 2015	FY 2016	FY 2017
Title: Assessing emerging COMSEC hardware and software systems and products (PL Net E)	0.107	1.074	1.170
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 strategic networks. (PL Net E) ***FY 2015 Accomplishments:*** Conduct a six month study of current and emerging cryptographic algorithms and technologies to identify strategies that will increase the longevity of cryptographic solutions. (PL Net E) ***FY 2016 Plans:*** Conduct testing of candidate small tactical In-line Network Encryption (INE) solutions and emerging secure wireless solutions. (PL Net E) ***FY 2017 Plans:*** As the Army implements new network technology, In-line Network Encryption (INE) devices must be identified and tested for effectiveness and suitability. Key areas of investigation include cyber security, interoperability, and standards compliance. (PL Net E)			
Title: The Defensive Cyberspace Operations (DCO) - Big Data Pilot (PL ES-CYBER)	-	9.725	-
Description: Bridge Big Data efforts into the DCO program and deploy additional Big Data Analytics platforms to FY15 JRSS sites. Assess alternative solution architecture/design and Develop, Test, Accredit, and Implement Rapid Deployable Kit (RDK) 2.X. (PL ES-CYBER) ***FY 2016 Plans:*** Big Data Pilot cyber funding encompasses beta testing and a validation plan that will be incorporated with the pilot effort. Includes expanded DCO and Cyberspace Situational Awareness program requirements. Candidate deployment locations based on FY15 JRSS site activations. (PL ES-CYBER)			
Title: Oversight and implementation guidance of emerging Cryptographic and IA capabilities to ensure interoperability to maintain compliance with DoD, NSA, and Army policies and regulations. (CIO/G6)	6.815	7.210	6.261
Description: The program provides oversight and guidance for technical research and evaluation of Cryptographic and Key Management capabilities to ensure IA compliance and interoperability. This effort improves operational effectiveness,			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
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 IA standards for new/modernized technology insertion to support the LWN 2025 and Beyond. This effort assesses and defines risk mitigation of IA network vulnerabilities in end-to-end Army network operations and Common Operating Environment. (CIO/G6) ***FY 2015 Accomplishments:*** This program researches new and emerging Cryptographic and IA technologies to bridge the operational gaps to enable secure communications between the tactical edge, the Army Enterprise Network and the DoD Joint Information Environment (JIE). Review operational needs, operation assessments, identify fundamental building blocks for IA solutions and risk reduction lab test commercial products for Army insertion. Participate in DOD pilot programs. Develop strategies and policies capitalizing on leveraging emerging cryptographic and key management technologies to enhance cyber security, prevent any undue risk and limitations and maximize performance to the Army networks. Effectively provide strategies, policies, and documentation to protect information, and knowledge sharing on the LandWarNet to secure the edge. Provide guidance for the adjustment of COMSEC programs and ensure COMSEC policies remains in synchronization with the latest COMSEC technologies. (CIO/G6) ***FY 2016 Plans:*** This COMSEC Modernization effort determines the maturity and viability of Cryptographic Key Management and IA technologies to ensure secure and interoperable National Security Systems and National Information. It provides increased operational availability, enhances Cyber posture, ensures performance based standards are consistent with COE and the DoD Joint Information Environment (JIE). Operational needs and assessments are reviewed and validated, identify fundamental building blocks for IA solutions and perform risk reduction testing of commercial products prior to insertion into Army for use. Exercise oversight to improve process and technical solutions before making investment strategy decisions so that duplications will be reduced or eliminated. Participate in operational assessment of NSA, DoD, Joint Staff and Service led Joint Capability Technology Demonstrations (JCTD) to align new technologies to documented Army and Service capability gaps for National Security Systems. Develop strategies and policies that leverage emerging cryptographic and key management tools and services. (CIO/G6) ***FY 2017 Plans:*** Oversight and Implementation guidance that provides a framework for Army Cryptographic Modernization and Key Management through the evaluation of performance, operational effectiveness, and operational suitability of advanced technologies to meet mission capability needs. The core functions of this program are to research and evaluate new emerging technology concepts for suitability and reliability participate in joint tests with NSA, DISA, and Services to establish functional and technical boundaries for Cryptographic Modernization, Key Management, and Cyber Security operations. The program resources Cybersecurity System of			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
Systems Network Vulnerability Assessments (CS SoS NVA) to assess vulnerabilities and determine the operational risks resulting from disruption, unauthorized access, modification or exploitation of the network, information and information systems.			
Accomplishments/Planned Programs Subtotals	6.922	18.009	7.431

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• DV5: *Crypto Modernization*	3.486	9.209	21.565	-	21.565	28.424	23.990	23.579	20.444	Continuing	Continuing
• ET9: *Embedded Crypto Modernization*	-	-	4.585	-	4.585	27.256	-	-	-	0	31.841
• B96002: *Cryptographic Systems*	18.151	16.206	66.692	-	66.692	28.820	32.765	70.685	101.519	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	-	3.014	-	3.014	33.896	58.047	58.014	27.825	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	1.721	2.530	2.545	-	2.545	2.635	3.170	4.917	4.961	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 increased, 19 Jun 15.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PL Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	78.009	0.107		1.074		1.170		-		1.170	Continuing	Continuing	Continuing
Big Data Pilot (PL ES-CYBER)	TBD	TBD : FT BELVOIR, VA	0.000	-		9.725		-		-		-	0	9.725	0
Information Assurance System Engineering Support (PL Net E)	C/FFP	DSCI Consulting : APG, MD	7.106	-		-		-		-		-	0	7.106	0
Engineering Support (PL Net E)	C/CPFF	CACI : APG, MD	5.018	-		-		-		-		-	0	5.018	Continuing
Engineering Support (PL Net E)	C/CPFF	Booz Allen Hamilton : APG, MD	3.408	-		-		-		-		-	0	3.408	0
Engineering Support (PL Net E)	C/FP	CSC : APG, MD	16.448	-		-		-		-		-	0	16.448	0
Engineering Support (CIO/G6)	C/FP	CACI : APG, MD	2.732	1.147		1.245		1.595		-		1.595	Continuing	Continuing	Continuing
System Engineering (CIO/G6)	SS/LH	CECOM RDEC : APG, MD	0.000	1.698		2.073		1.086		-		1.086	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/CPFF	Booz Allen Hamilton : APG, MD	2.807	1.756		1.625		1.261		-		1.261	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/FFP	AASKI : Edgewood, MD	0.000	1.032		1.079		1.316		-		1.316	Continuing	Continuing	Continuing
Service (CIO/G6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	2.164	1.182		1.188		1.003		-		1.003	Continuing	Continuing	Continuing
		Subtotal	117.692	6.922		18.009		7.431		-		7.431	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support (PD Net E)	C/CPFF	TBD : TBD	1.598	-		-		-		-		-	0	1.598	0

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Army		Date: February 2016
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 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	1.598	-		-		-		-		-	0.000	1.598	0.000

Remarks

Not Applicable

	Prior Years	FY 2015		FY 2016		FY 2017 Base		FY 2017 OCO		FY 2017 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	119.290	6.922		18.009		7.431		-		7.431	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

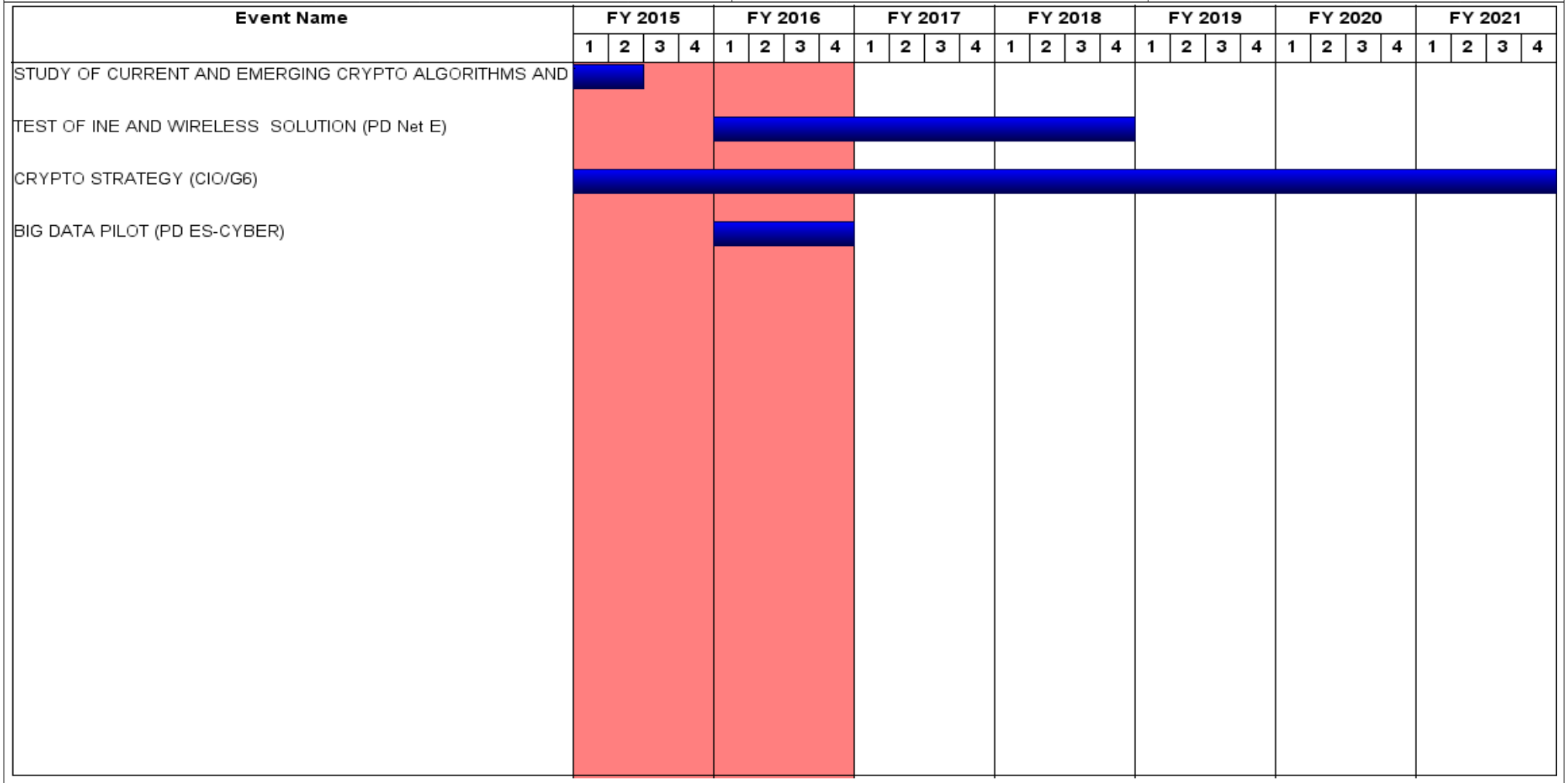

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
STUDY OF CURRENT AND EMERGING CRYPTO ALGORITHMS AND TECHNOLOGIES (PD Net E)	1	2015	2	2015
TEST OF INE AND WIRELESS SOLUTION (PD Net E)	1	2016	4	2018
CRYPTO STRATEGY (CIO/G6)	1	2014	4	2021
BIG DATA PILOT (PD ES-CYBER)	1	2016	4	2016

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 501 / *Army Key Mgt System*	

COST ($ in Millions)	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
501: *Army Key Mgt System*	-	1.138	1.927	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	3.065
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Army Key Management System (AKMS) (501) realigned to Key Management Infrastructure (KMI)PE/Project (373140)(DV4) in FY17.

A. Mission Description and Budget Item Justification

The Army Key Management System (AKMS) is the Army's implementation of the National Security Agency's (NSA) Electronic Key Management System (EKMS) program automating the functions of Communications Security (COMSEC) electronic key management, control, planning, and distribution. AKMS 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 AKMS System of Systems (SoS) components are the Local COMSEC Management Software (LCMS), Automated Communications Engineering Software (ACES) and Simple Key Loader (SKL).

The NSA EKMS program is being replaced by the NSA Key Management Infrastructure (KMI) Program. The transition of the legacy EKMS LCMS to the modern KMI Management Client Nodes (MGC)s began in FY12 and must be completed by the EKMS Tier 2 sunset date of December 2017.

AKMS supports the transition to Army Key Management Infrastructure (AKMI). Some components of the AKMS SoS will be replaced under AKMI while others will be modified or adapted to meet the new AKMI requirements. Two critical components required for the transition include the development of the Mission Planning Management Support System (MPMSS) and the ability to support Over the Network Keying (OTNK).

MP/MSS creates a secure, highly automated interface enabling secure transparent provisioning of KMI products. MP/MSS service is being developed by NSA but each Service is responsible for interface development and final integration into their infrastructure. ACES is the initial target for the interface to MPMSS. NSA will be providing additional capabilities and updates to the MP/MSS interface specification through technology insertions in the out years. The Army must then adjust to these changes delivered by NSA.

One of the major enhancement in the KMI architecture is the ability to leverage OTNK. 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 from the tactical edge up through strategic ECU's. Within AKMS this capability will be focused on ACES and SKL platform. ACES and SKL will act as an interim solution for all legacy ECUs to be recognized on the KMI network until they can be upgraded to be fully KMI aware. OTNK developments began in FY2015.

To support this transition, a new KMI compliant cryptographic engine must be developed for the SKL platform. The KOV-21 card used in current Army Tier 3 fill devices has hardware obsolescence issues and does not support the new capabilities being delivered by KMI. Redesigning and developmental efforts using modern and readily

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

available components for use in the Army's SKL devices have been initiated. 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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
Title: Mission Planning Management Support System (MPMSS) Interface	1.138	1.021	-
Description: The Mission Planning Management Support System (MPMSS) creates a secure, highly automated interface to enable transparent provisioning of Key Management Infrastructure (KMI) products. The MPMSS system is to be used by both the KMI system developer and MPMSS developers to have a standard interface to electronically exchange information, enabling Warfighter Operations, achieving integration between provisioning. NSA plans to deliver the MPMSS capabilities in 4 releases; Spirals 1-4, through FY17. ***FY 2015 Accomplishments:*** The first functional capability release of MPMSS will be completed in KMI Spiral 2 Spin 2 scheduled for delivery in July 2015. This release will include the 1) KMI product ordering, 2) distribution management and the Spin 1 backlog. This installment will make it easier for the KMI Operating Account Manager (KOAM) to locally generate key for incoming requests where the key is not already on-hand. Additionally, this release will virtualize all needed components for MPMSS. The development of the Army Mission Planner software that will interface with the KMI MPMSS API will begin FY15 and be carried out through FY18. The Army Mission Planner software will be integrated and tested with the KMI MPMSS API Spin 2 capabilities. ***FY 2016 Plans:*** The second functional capability release of MPMSS will be completed in KMI Spiral 2 Spin 3 scheduled for delivery in July 2016. This release will include the interface to support the initial certificate management services. The Army Mission Planner software will be integrated and tested with the KMI MPMSS API Spin 3 capabilities. These installments of the MPMSS effort are a continuing effort to the base capabilities developed in the Army Key Management System (AKMS) program and will ensure maximum use of KMI architecture by Army's legacy ECUs. This effort will commence after KMI MP/MSS software code is completed and delivered to the Army.			
Title: Key Management Infrastructure (KMI) Awareness for Legacy Devices	-	0.906	-
Description: KMI Awareness initiative creates a secure, highly automated interface in providing future Over the Network Keying (OTNK) capability to legacy End Crypto Units (ECUs). This initiative will allow KMI aware ECUs to receive, authenticate, and decrypt OTNK messages and increases WarFighter survivability by minimizing the need for Soldiers to travel to obtain keys. The current army inventory of ~1.5M ECUs are not currently KMI aware and cannot perform OTNK functionality. ***FY 2016 Plans:*** KMI Awareness initiative provides OTNK like capability to legacy ECUs through the fill device. Development of a Reprogrammable Single Chip Universal Encryptor (RESCUE) is necessary for the fill device to provide KMI aware services to the			

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
ECUs. Developing this capability in the SKL will allow the ~1.5M legacy ECUs to be recognized on the KMI network until they can be upgraded to be KMI aware.			
Accomplishments/Planned Programs Subtotals	1.138	1.927	-

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• BA1201: *TSEC - AKMS*	10.382	10.373	-	-	-	-	-	-	-	0	20.755
• B96004: *Key Management Infrastructure*	41.113	45.678	63.578	-	63.578	58.981	92.898	94.813	96.399	Continuing	Continuing
• DV4: *Key Management Infrastructure*	2.081	2.009	4.699	-	4.699	4.782	3.333	-	3.395	Continuing	Continuing
• 432140: *ISSP (TSEC-AKMS)*	4.047	7.380	8.006	-	8.006	8.316	8.678	3.945	4.043	Continuing	Continuing

Remarks

Line Item & Title:
BA1201: TSEC-AKMS (OPA2)
B96004: Key Management Infrastructure (OPA2)
DV4: Key Management Infrastructure (RDTE)
432140: ISSP (TSEC-AKMS) (OMA)

D. Acquisition Strategy

Army Key Management System (AKMS) is an ACAT III Program of Record (POR) under PL Network Enablers (PL Net E). It is the Army's implementation of the National Security Agency (NSA)'s Electronic Key Management System (EKMS). The AKMS allows the Army to manage, control, plan, and distribute electronic key for the ~1.5 million End Cryptographic Units (ECU)s necessary to communicate and distribute data on the Army's tactical and strategic networks.

AKMS was initially approved for Milestone III in FY99. The AKMS System of Systems originally included Local COMSEC Management Software (LCMS), Automated Communications Engineering Software (ACES) and Data Transfer Device (DTD) (AN-CYZ-10). In 2QFY02, the PEO C3T Milestone Decision Authority approved the procurement of the Simple Key Loader (SKL) as the replacement for the DTD within the AKMS System of Systems (SoS) POR. AKMS is a fully fielded POR that undergoes modifications to meet emerging operational needs.

The NSA EKMS program is being replaced by the NSA Key Management Infrastructure (KMI) Program. As the DoD Key Management Lead, NSA is dictating the change from EKMS to KMI. The Army's implementation of the NSA KMI is the Army Key Management Infrastructure (AKMI) program. Some components of the AKMS SoS will be replaced under AKMI while others will be modified or adapted to meet the new AKMI requirements.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

The LCMS component of the AKMS SoS (AN/GYK-49) is fully fielded. The LCMS is assigned to the COMSEC Account Manager/COMSEC Custodian. LCMS most recent hardware refresh was completed in FY12. The current software baseline is 5.1.0.5 with certain select accounts upgrading to v5.2 based on operational needs. Further LCMS software releases are not anticipated. LCMS workstations will be replaced by KMI Management Client (MGC) Nodes before the NSA mandated EKMS Tier 2 sunset of December 2017. EKMS Common Tier 1 operations and Tier 1 operational support continues to be provided by CECOM. LCMS hardware is sustained by CSLA until fully replaced by the KMI MGC.

The ACES component of the AKMS SoS (AN/GYK-33) current hardware platform is a Dell E6500 non-ruggedized laptop fielded to S6, Spectrum Managers and some COMSEC Account Managers at Battalion level and above. ACES is undergoing a hardware technology refresh and will be replacing 1/5 quantity of laptops each year. The current version of ACES is 3.4. Software is released on an annual basis and coincides with the Capability Set delivery schedule. PL Net E currently holds the software development contract. As the Tier 2.5 component, ACES operates between the LCMS (Tier 2) and the SKL (Tier 3). It links the key data from the LCMS with mission planning data for a single load by the SKL into the ECUs. ACES will continue with modifications to support the AKMI System of Systems. In order to support AKMI, ACES must be modified to seamlessly operate within the KMI architecture.

The SKL is the primary Army fill device and is the Tier 3 component of the AKMS SoS (AN/PYQ-10). The SKL is fully fielded to the Army. Army holds the sole full rate production procurement contract for the SKL, which is heavily utilized by other DoD and civil services as well as FMS customers. The SKL repair capability is with the Original Equipment Manufacturer but TYAD is developing an organic depot repair support. The SKL and its cryptographic engine are facing hardware obsolescence issues. SKL v3.1 in combination with a new KMI compliant cryptographic engine resolves these issues and lays the foundation for the Army's Next Generation Load Device- Medium capability. The SKL v3.1 modifications will be made to the Army's existing fleet of the fill devices via a modification kit starting in FY15. The KMI cryptographic engine is reliant on the CERDEC-led RESCUE RDT&E effort that began in FY14.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Army			Date: February 2016
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 501 / *Army Key Mgt System*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MPMSS	MIPR	NSA : Linthicum, MD	2.807	-		-		-		-		-	0	2.807	0
MPMSS Army Interface	MIPR	TBD : APG, MD	0.000	1.138		1.021		-		-		-	0	2.159	0
KMI Awareness for Legacy Devices	C/CPFF	CERDEC S&TCD : APG, MD	0.000	-		0.906		-		-		-	0	0.906	0
		Subtotal	2.807	1.138		1.927		-		-		-	0.000	5.872	0.000

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	2.539	-		-		-		-		-	0	2.539	0
		Subtotal	2.539	-		-		-		-		-	0.000	2.539	0.000

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	2.683	-		-		-		-		-	0	2.683	0
		Subtotal	2.683	-		-		-		-		-	0.000	2.683	0.000

	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	8.029	1.138		1.927		-		-		-	0.000	11.094	0.000

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

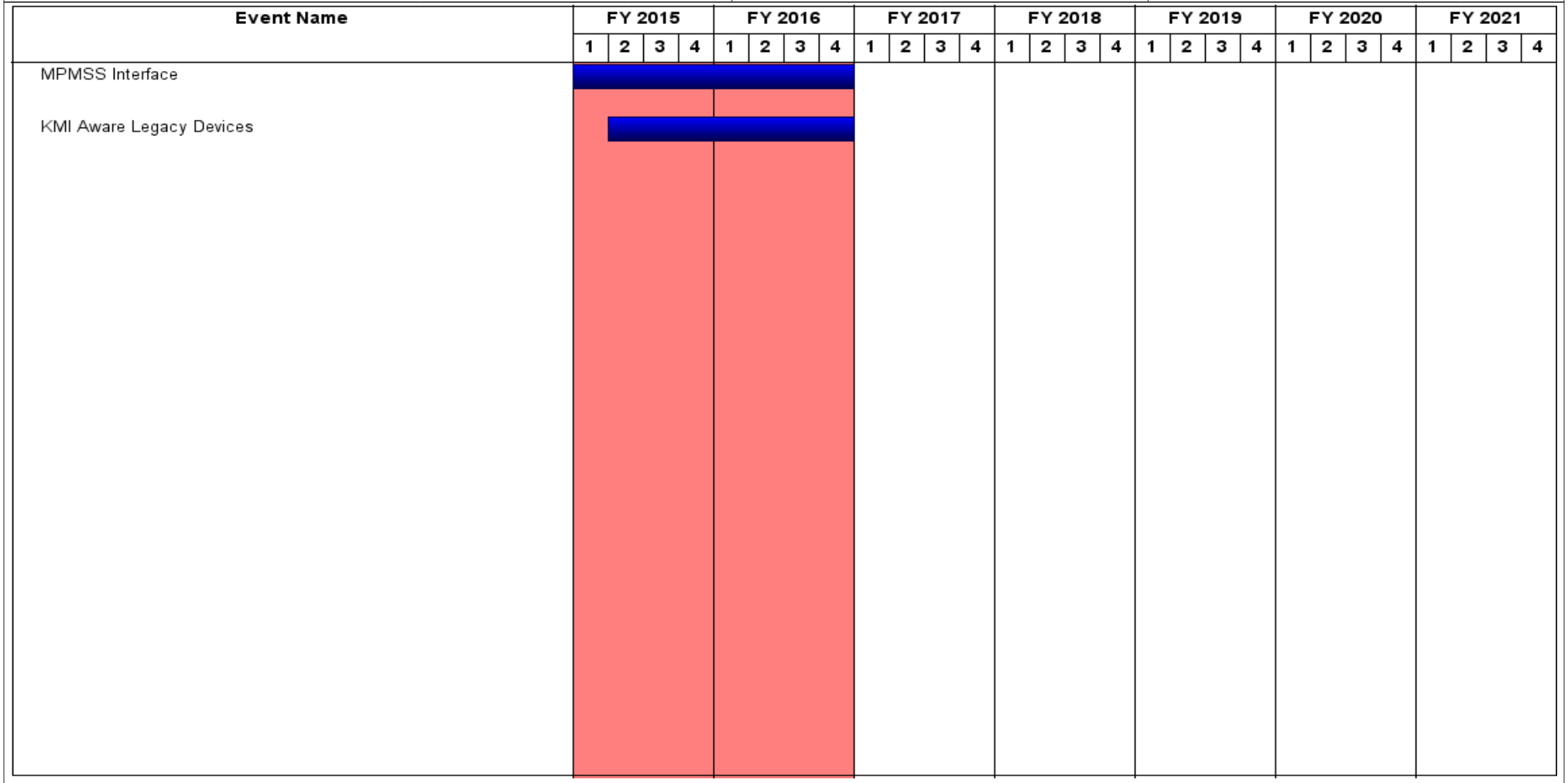

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
MPMSS Interface	1	2013	4	2016
KMI Aware Legacy Devices	2	2015	4	2016

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
DV4: *Key Management Infrastructure (KMI)*	-	2.081	2.009	4.699	-	4.699	4.782	3.333	0.000	3.395	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Key Management Infrastructure (KMI) (DV4) was realigned from project 491 in FY2014. Army Key Management System (AKMS) (501) realigned to Key Management Infrastructure (KMI) (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 Crypto Modernization Initiatives 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), 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 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 Cryptographic Modernization Initiatives (CMI).

One of the major enhancement in the AKMI architecture is the ability for 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 from 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 and Large are 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 redesign of 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.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
Title: Key Management Infrastructure (KMI) Awareness (RESCUE / KOV-21 Replacement Effort)	2.081	2.009	4.699
Description: KMI Awareness initiative creates a secure, highly automated interface in providing future Over the Network Keying (OTNK) capability to legacy End Crypto Units (ECUs). 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 2015 Accomplishments:*** The Reprogrammable Single Chip Universal Encryptor (RESCUE) technology development effort will be led by the Army Communications-Electronics Research Development and Engineering Center (CERDEC) Space and Terrestrial Communications Directorate (S&TCD) in coordination with the Army Program Executive Office for Command, Control, and Communications Tactical (PEO C3T) Product Director Network Enablers (PL Net E). The RESCUE effort is focused on the development, maturation, evaluation, and certification of the technology needed to meet the requirements of NSA and the Army. The RESCUE technology can be reused, scaled, and/or repackaged to satisfy the cryptographic requirements for other programs/platforms requiring or needing a KMI aware or Product Delivery Enclave (PDE) enabled solution. The KOV-21 replacement will be developed to be compatible with and installed in the SKL v3.1 to meet the Army's NGLD Medium requirement. The KOV-21 replacement will also be used in the future Army NGLD Large device. ***FY 2016 Plans:*** The RESCUE technology development will continue in FY2016. 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 2017 Plans:*** The RESCUE technology development will complete in FY2017. 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.			
Accomplishments/Planned Programs Subtotals	2.081	2.009	4.699

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*	

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	41.113	45.678	63.578	-	63.578	58.981	92.989	94.813	96.399	Continuing	Continuing
• BA1201: *TSEC - Army Key Mgt Sys (AKMS)*	10.382	10.373	-	-	-	-	-	-	-	0	20.755
• 501: *Army Key Management System (AKMS)*	1.138	1.927	-	-	-	-	-	-	-	0	3.065
• 432140: *ISSP (TSEC-AKMS)*	4.047	7.385	8.006	-	8.006	8.316	8.678	3.945	4.043	Continuing	Continuing

Remarks

Line Item & Title:
B96004: Key Management Infrastructure (OPA2)
BA1201: TSEC-Army Key Mgt Sys (AKMS) (OPA2)
501: Army Key Management System (AKMS) (RDTE)
432140: ISSP (TSEC-AKMS) (OMA)

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) is a Non Program of Record (POR) under PD Network Enablers (PL Net E). AKMI is the Army's implementation of the National Security Agency (NSA) Key Management Infrastructure (KMI) ACAT IAM Program of Record. The AKMI will allow the Army to manage, control, plan, and distribute electronic key for the ~1.5 million End Cryptographic Units (ECU)s necessary to communicate and distribute data on the Army's tactical and strategic networks.

AKMI initial Army Acquisition Program Baseline (APB) was approved 2QFY12. The AKMI Program will include the Management Clients (MGC), 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 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 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

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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)*

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 FY18. Additionally, the Army NGLD large strategy is highly reliant on the development of the RESCUE and will drive a final acquisition decision in FY18.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Army			Date: February 2016
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
KMI Awareness (RESCUE / KOV-21 Replacement Effort)	C/CPFF	CERDEC, S&TCD : APG, MD	0.000	2.081		2.009		4.699		-		4.699	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CERDEC, S&TCD : APG, MD	1.451	-		-		-		-		-	0.000	1.451	Continuing
		Subtotal	1.451	2.081		2.009		4.699		-		4.699	-	-	-

	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	1.451	2.081		2.009		4.699		-		4.699	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Army		Date: February 2016
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)*

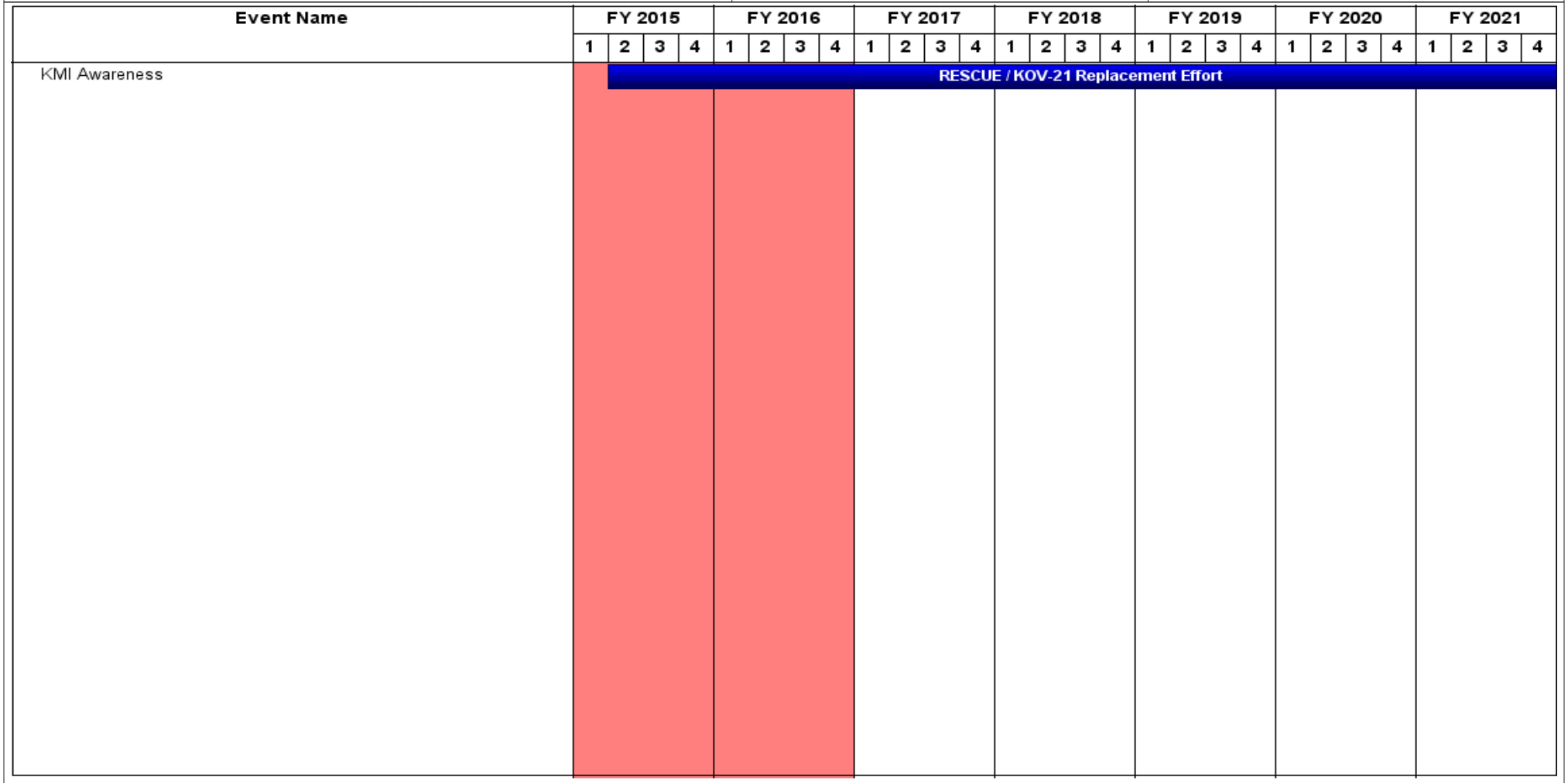

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
KMI Awareness	2	2015	4	2021

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	3.486	9.209	21.565	-	21.565	28.424	23.990	23.579	20.444	Continuing	Continuing
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 National Network Enterprise in as transparent a manner as possible.

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 employs embedded cryptographic hardware will be able to accept and utilize modern cryptographic key.

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 Information Assurance (IA) networked vulnerabilities to National information security systems. CDD, approved 15 Jul 10; ICD, approved 25 Mar 11; AAO; approved 15 Dec 11 and increased, 19 Jun 15.

FY17 $10.659M from the RDT&E line 0303140A-DV5 is required for a planned 4QFY17 solicitation of the ECMI development contracts, obligation of planned prior year funding expected 1QFY18 with contract awards.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.500	0.500	0.500

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
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 2015 Accomplishments:*** The program will test and evaluate Low Rate Initial Production (LRIP) of VACM 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. ***FY 2016 Plans:*** The program will test and evaluate engineering changes to Low Rate Initial Production (LRIP) 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. ***FY 2017 Plans:*** The program will continue to test and evaluate engineering changes to Low Rate Initial Production (LRIP) 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.			
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 can be performed on hardware, software, or network systems. ***FY 2015 Accomplishments:*** The program tests and evaluates COMSEC devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. Tests interfaces and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluates performance of	2.986	3.179	4.314

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
technologies and provide direction on were technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2016 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, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. Tests interfaces and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluates performance of technologies and provide direction on where technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data. ***FY 2017 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, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. Tests interfaces and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluates performance of technologies and provide direction on where technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data. Examples of common analysis to be performed are comparisons in encryption implementations, network initialization overhead, and comparison of emerging Commercial Solutions for Classified architectures with COMSEC architectures.			
Title: High Assurance Internet Protocol Encryption (HAIPE) extension manager ***Description:*** A management tool to configure the new extensions to the High Assurance Internet Protocol Encryption (HAIPE) standard and process the resulting data to provide early indications of cyber attacks. ***FY 2017 Plans:*** Conduct a software development effort 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 upgrade Army HAIPEs to include new cyber-sensor functionality for the tactical cyber cell.	-	-	1.503
Title: Embedded Cryptographic Modernization Initiative	-	5.530	-

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017
Description: The Embedded Cryptographic Modernization Initiative conducts research and analysis to determine optimal algorithms and engineering approaches to modernizing various cryptographic modules that are embedded within Army communications systems and data links. The analysis will follow a complete life cycle approach including factors relating to fielding, training, and sustainment as well as technical factors to ensure efficiently meeting of cease key dates while minimizing cost. ***FY 2016 Plans:*** The Embedded Cryptographic Modernization Initiative includes research and analysis to determine optimal algorithms and engineering approaches to modernizing various embedded cryptographic modules within Army communications systems and data links. The analysis will follow a complete life cycle approach including factors relating to fielding, training, and sustainment as well as technical factors to ensure compliance with NSA mandated cease key dates, while minimizing cost. Once approaches are identified, the necessary non-recurring testing, engineering and development of hardware and software will be completed. Any necessary production will begin. Detailed fielding and training plans will be developed for each solution.			
Title: Embedded Cryptographic Modernization Initiative Govt Purpose Rights Software Upgrade ***Description:*** Software engineering and coding to upgrade the government purposed rights software code used in software defined radios to ensure these radios remain secure by employing algorithms and keys that comply with CJCSI 6510. ***FY 2017 Plans:*** Update software specification, software design, software coding, and develop test plan.	-	-	4.589
Title: Embedded Cryptographic Modernization Initiative Development Contracts ***Description:*** Non Recurring Engineering (NRE) contracts to comply with cease key dates mandated by CJCSI 6510. ***FY 2017 Plans:*** 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, and functional allocation. Design of modern reprogrammable cryptographic modules. Detailed hardware design and software coding.	-	-	10.659
Accomplishments/Planned Programs Subtotals	3.486	9.209	21.565

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	6.922	18.009	7.431	-	7.431	10.092	8.783	9.228	9.814	Continuing	Continuing
• ET9: *Embedded Crypto Modernization*	-	-	4.585	-	4.585	27.256	-	-	-	0.000	31.841
• B96002: *Cryptographic Systems*	18.151	16.206	66.692	-	66.692	28.820	32.765	70.685	101.519	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	-	3.014	-	3.014	33.896	58.047	58.014	27.825	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	1.721	2.530	2.545	-	2.545	2.635	3.170	4.917	4.961	Continuing	Continuing

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by 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 Information Assurance (IA) networked vulnerabilities to National 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 increased, 19 Jun 15.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Army			Date: February 2016
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CECOM RDEC : APG, MD	0.340	0.932		0.945		1.682		-		1.682	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	0.359	1.578		1.725		2.839		-		2.839	Continuing	Continuing	0
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.215	0.235		0.245		0.436		-		0.436	Continuing	Continuing	0
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	0.358	0.613		0.625		1.113		-		1.113	Continuing	Continuing	0
Information Assurance System Engineering Support	C/FFP	DSCI : Aberdeen, Maryland	0.115	0.128		0.139		0.247		-		0.247	Continuing	Continuing	0
Embedded Crypto Modernization Support	C/LH	TBD : TBD	0.000	-		5.530		-		-		-	0.000	5.530	0
ECMI Development Contracts	C/CPFF	TBD : TBD	0.000	-		-		10.659		-		10.659	0	10.659	0
ECMI GPR SW upgrade	C/CPFF	TBD : TBD	0.000	-		-		4.589		-		4.589	0	4.589	0
		Subtotal	1.387	3.486		9.209		21.565		-		21.565	-	-	-

	Prior Years	FY 2015		FY 2016		FY 2017 Base		FY 2017 OCO		FY 2017 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	1.387	3.486		9.209		21.565		-		21.565	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Army		Date: February 2016
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)*

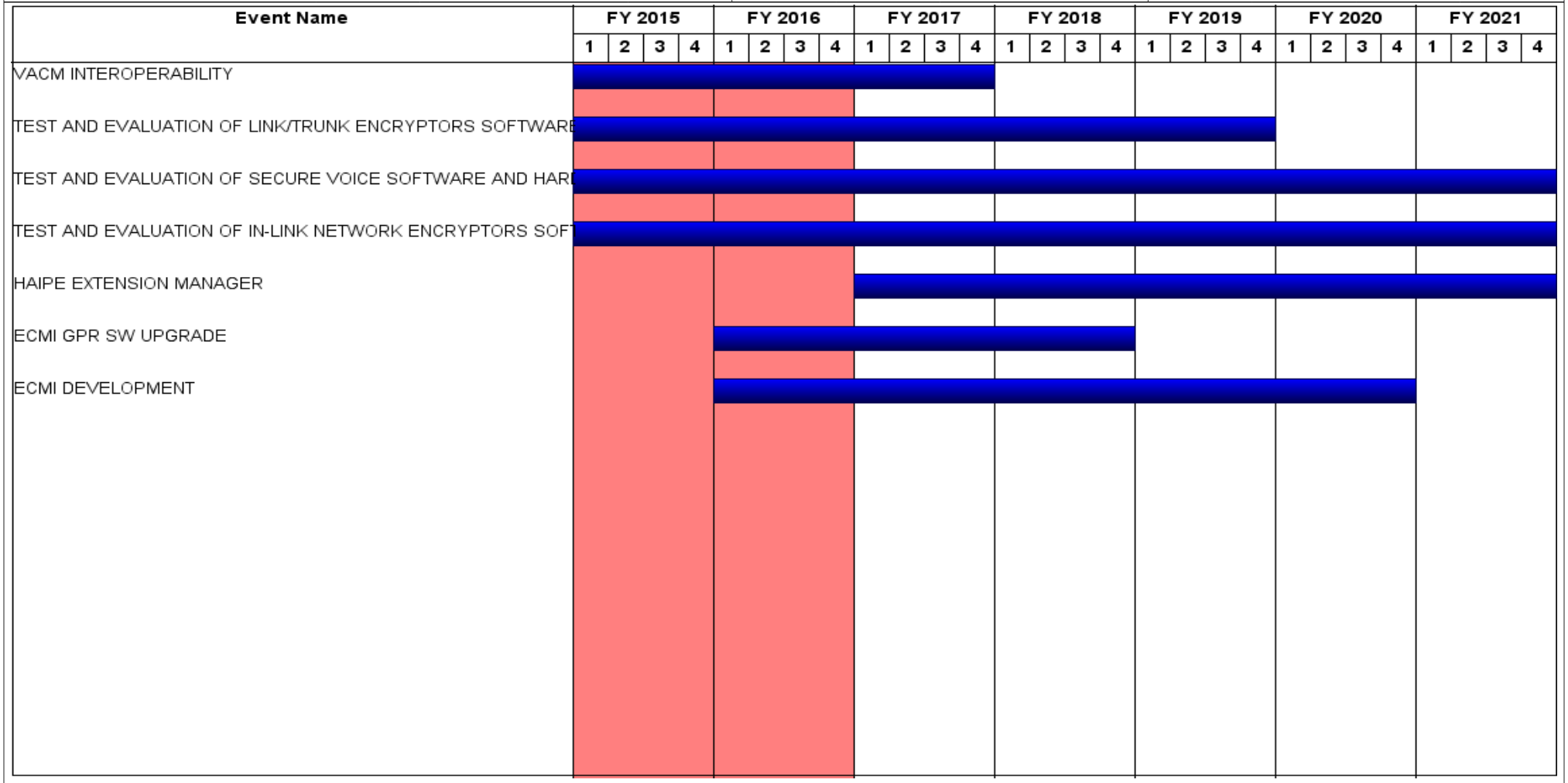

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
VACM INTEROPERABILITY	4	2013	4	2017
TEST AND EVALUATION OF LINK/TRUNK ENCRYPTORS SOFTWARE	4	2013	4	2019
TEST AND EVALUATION OF SECURE VOICE SOFTWARE AND HARDWARE	4	2013	4	2021
TEST AND EVALUATION OF IN-LINK NETWORK ENCRYPTORS SOFTWARE & HARDWARE	4	2013	4	2021
HAIPE EXTENSION MANAGER	1	2017	4	2021
ECMI GPR SW UPGRADE	1	2016	4	2018
ECMI DEVELOPMENT	1	2016	4	2020

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	0.000	0.000	4.585	-	4.585	27.256	0.000	0.000	0.000	0.000	31.841
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

ET9 – The Embedded Crypto Modernization 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 enduring Army radios remain secure by operating with modern crypto keys. Tactical radios using embedded cryptographic systems will no longer be able to communicate securely after Crypto Keys expire due to 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 modernize their cryptographic capabilities by implementing the modern algorithms. If cease key dates are not met, Army will be forced to communicate at risk.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2015	FY 2016	FY 2017
Title: Embedded Cryptographic Modernization Initiative	-	-	4.585
Description: ECMI Non Recurring Engineering (NRE) Contract Prep Work ***FY 2017 Plans:*** Contract Prep Work to include RFP, SOW and contract award for 4QFY17 ECMI Development. PMO will conduct research and analysis to determine optimal algorithms and engineering approaches to modernize various cryptographic modules that are embedded within Army tactical radios.			
Accomplishments/Planned Programs Subtotals	-	-	4.585

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	6.922	18.009	7.431	-	7.431	10.092	8.783	9.228	9.814	Continuing	Continuing
• DV5: *Crypto Modernization*	3.486	9.209	21.565	-	21.565	28.424	23.990	23.579	20.444	Continuing	Continuing
• B96002: *Cryptographic Systems*	18.151	16.206	66.692	-	66.692	28.820	32.765	70.685	101.519	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2017 Army		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• B96006: *Embedded Cryptographic Modernization*	-	-	3.014	-	3.014	33.896	58.047	58.014	27.825	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	1.721	2.530	2.545	-	2.545	2.635	3.170	4.917	4.961	Continuing	Continuing

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by 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 Cryptographic Systems 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 systems. ECMI will design, develop, and execute upgrade activities to ensure all enduring Army tactical radios that employs embedded cryptographic hardware will be able to accept and utilize modern cryptographic keys.

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 2017 Army			Date: February 2016
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)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PD Net-E Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	0.000	-		-		2.837		-		2.837	0	2.837	0
PM TR Program Mgmt Personnel	C/CPFF	BAH : Aberdeen, MD	0.000	-		-		1.424		-		1.424	0	1.424	0
PM TR Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	0.000	-		-		0.324		-		0.324	0	0.324	0
		Subtotal	0.000	-		-		4.585		-		4.585	0.000	4.585	0.000

	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	-		0.000		4.585		-		4.585	0.000	4.585	0.000

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Army		Date: February 2016
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)*

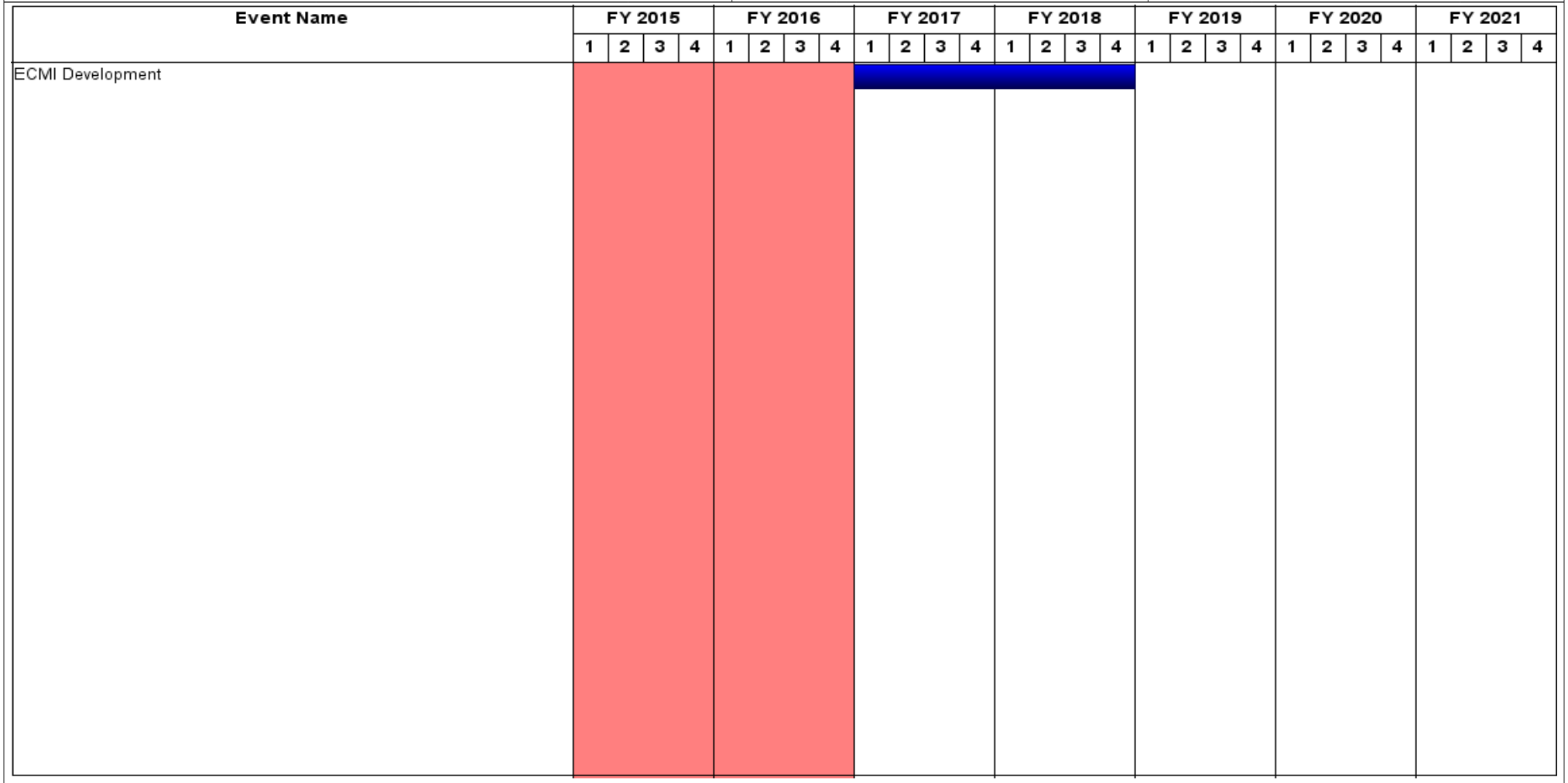

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Army		Date: February 2016
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
ECMI Development	1	2017	4	2018