Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Army											Date: February 2015	
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**Cost To Complete**	**Total Cost**
Total Program Element	-	9.040	14.167	31.154	-	31.154	25.687	26.316	24.272	6.871	Continuing	Continuing
491: *Information Assurance Development*	-	4.940	7.197	18.009	-	18.009	8.670	8.971	7.403	-	-	55.190
501: *Army Key Mgt System*	-	1.262	1.183	1.927	-	1.927	2.328	2.568	-	-	-	9.268
DV4: *Key Management Infrastructure (KMI)*	-	1.451	2.163	2.009	-	2.009	2.382	2.214	3.333	-	-	13.552
DV5: *Crypto Modernization (Crypto Mod)*	-	1.387	3.624	9.209	-	9.209	12.307	12.563	13.536	6.871	Continuing	Continuing

Note

In FY16 the following adjustments were made:

The FY16 funding request was reduced by $2.235 million to account for the availability of prior year funding execution balances.

Information Assurance funding was increased by $9.725 million in support of defensive cyberspace operations.
Crypto Modernization funding was increased by $4.441 million in support of the embedded cryptographic modernization initiative.

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 supports the technical assessment and specifications documentation of cryptographic, key management and 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. 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 in accordance with the Army Network Campaign Plan. This will be accomplished by

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Army	Date: February 2015
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*

interoperability, 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 NSA Electronic Key Management System (EKMS) program automating the functions of COMSEC electronic key management, control, planning, and distribution. 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 NSA EKMS program is being replaced by the NSA Key Management Infrastructure (KMI) Program. 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 transition of the legacy EKMS LCMS to the modern KMI Management Client Nodes (MGC)s began in FY12 and must be completed by the LCMS sunset date of December 2017. AKMS supports the transition to AKMI.

The Army Key Management Infrastructure (AKMI) is the Army's implementation of the NSA KMI ACAT IAM Program. KMI further automates the functions of 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 C4I systems. KMI provides an integrated, operational environment that brings essential key management functions in-band. AKMI supports Department of Defense (DoD) Global Information Grid (GIG) Net Centric and Crypto Modernization Initiatives and supports emerging key management requirements. AKMI achieves an Over the Network Keying (OTNK) solution to support emerging cryptographically modernized systems. Some components of the AKMS SoS will be replaced under AKMI while others will be modified or adapted to meet the new KMI requirements. The AKMI SoS includes the MGC Nodes, ACES and the NGLD Family.

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. The Cryptographic Modernization Initiative (CMI) is designed to investigate Courses Of Action (COAs), conduct a Material Solution Analysis (MSA), 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Army					Date: February 2015
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*			
B. Program Change Summary ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Previous President's Budget	9.351	14.175	19.054	-	19.054
Current President's Budget	9.040	14.167	31.154	-	31.154
Total Adjustments	-0.311	-0.008	12.100	-	12.100
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-0.008			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.311	-			
• Adjustments to Budget Years	-	-	0.169	-	0.169
• Underexecution Reduction	-	-	-2.235	-	-2.235
• Defensive Cyberspace Ops	-	-	9.725	-	9.725
• Embedded Crypto Modernization Initiative	-	-	4.441	-	4.441

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army											Date: February 2015	
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**Cost To Complete**	**Total Cost**
491: *Information Assurance Development*	-	4.940	7.197	18.009	-	18.009	8.670	8.971	7.403	-	-	55.190
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

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

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. (PD Net E)

Funding supports the technical assessment and specifications documentation 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. (CIO/G6)

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, 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. (CIO/G6)

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 2016 Army		Date: February 2015
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. (PD ES-CYBER)

B. Accomplishments/Planned Programs ($ in Millions)	FY 2014	FY 2015	FY 2016
Title: Assessing emerging COMSEC hardware and software systems and products (PD 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 strategic networks. (PD Net E) ***FY 2015 Plans:*** Conduct a six month study of current and emerging cryptographic algorithms and technologies to identify strategies that will increase the longevity of cryptographic solutions. (PD Net E) ***FY 2016 Plans:*** Conduct testing of candidate small tactical In-line Network Encryption (INE) solutions and emerging secure wireless solutions. (PD Net E)	-	0.112	1.074
Title: Cryptographic Systems Test and Evaluation (PD Net E) ***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. (PD Net E) ***FY 2014 Accomplishments:*** The program tests and evaluates systems 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 tests and evaluates 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. Develops 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 were technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data. (PD Net E)	1.848	-	-
Title: The Defensive Cyberspace Operations (DCO) - Big Data Pilot (PD ES-CYBER)	-	-	9.725

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
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. (PD 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. (PD 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) ***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, 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 2014 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 and assessments, identify fundamental building blocks for IA solutions and provide risk reduction lab tests commercial products that are designated for Army insertion. Participate in DOD pilot programs that develop strategies and policies that capitalize on leveraging emerging cryptographic and key management technologies to enhance cyber security and maximize performance to the Army networks. Provide strategies, policies, and documentation to protect information, and knowledge sharing on the LandWarNet to secure the edge. Provide policies and guidance for all COMSEC programs and initiatives to ensure capabilities, interoperability, suitability remains in synchronized with Army requirements. (CIO/G6) ***FY 2015 Plans:*** 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	3.092	7.085	7.210

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
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)			
Accomplishments/Planned Programs Subtotals	4.940	7.197	18.009

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• DV5: *Cryptographic Systems RDTE*	1.387	3.624	9.209	-	9.209	12.307	12.563	13.536	6.871	Continuing	Continuing
• TA0600: *Information System Security Program - ISSP*	13.245	-	19.920	-	19.920	-	-	-	-	-	33.165
• B96002: *Cryptographic Systems OPA2*	4.334	18.151	16.206	-	16.206	33.006	59.781	48.658	64.961	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	-	3.521	2.530	-	2.530	2.574	2.656	3.197	4.956	Continuing	Continuing

Remarks

0303140A DV5 - Cryptographic System - RDTE funds
TA0600 - Information System Security Program - OPA2 funds
B96002 - Cryptographic Systems - OPA2 funds
BS9716 - NON PEO-SPARES - OPA4 funds

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

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. CDD, approved by CIO/G6, 15 Jul 10; ICD, approved by JROC, 25 Mar 11; AAO; approved by G3, 15 Dec 11.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2016 Army			Date: February 2015
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 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PD Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	74.141	0.672		0.112		1.074		-		1.074	Continuing	Continuing	Continuing
Big Data Pilot (PD ES-CYBER)	TBD	TBD : FT BELVOIR, VA	0.000	-		-		9.725		-		9.725	-	9.725	-
Information Assurance System Engineering Support (PD Net E)	C/FFP	DSCI Consulting : APG, MD	6.881	0.225		-		-		-		-	-	7.106	-
Engineering Support (PD Net E)	C/CPFF	CACI : APG, MD	4.515	0.503		-		-		-		-	Continuing	Continuing	Continuing
Engineering Support (PD Net E)	C/CPFF	Booz Allen Hamilton : APG, MD	3.064	0.344		-		-		-		-	-	3.408	-
Engineering Support (PD Net E)	C/FP	CSC : APG, MD	16.448	-		-		-		-		-	-	16.448	-
Engineering Support (CIO/G6)	C/FP	CACI : APG, MD	1.513	1.219		1.147		1.245		-		1.245	Continuing	Continuing	Continuing
System Engineering (CIO/G6)	SS/LH	CECOM RDEC : APG, MD	0.000	-		1.973		2.073		-		2.073	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/CPFF	Booz Allen Hamilton : APG, MD	1.530	1.277		1.751		1.625		-		1.625	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/FFP	AASKI : Edgewood, MD	0.000	-		1.032		1.079		-		1.079	Continuing	Continuing	Continuing
Service (CIO/G6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	1.464	0.700		1.182		1.188		-		1.188	Continuing	Continuing	Continuing
		Subtotal	109.556	4.940		7.197		18.009		-		18.009	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support (PD Net E)	C/CPFF	TBD : TBD	1.598	-		-		-		-		-	-	1.598	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2016 Army			Date: February 2015
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 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	1.598	-		-		-		-		-	-	1.598	-

Remarks

Not Applicable

	Prior Years	FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	111.154	4.940		7.197		18.009		-		18.009	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

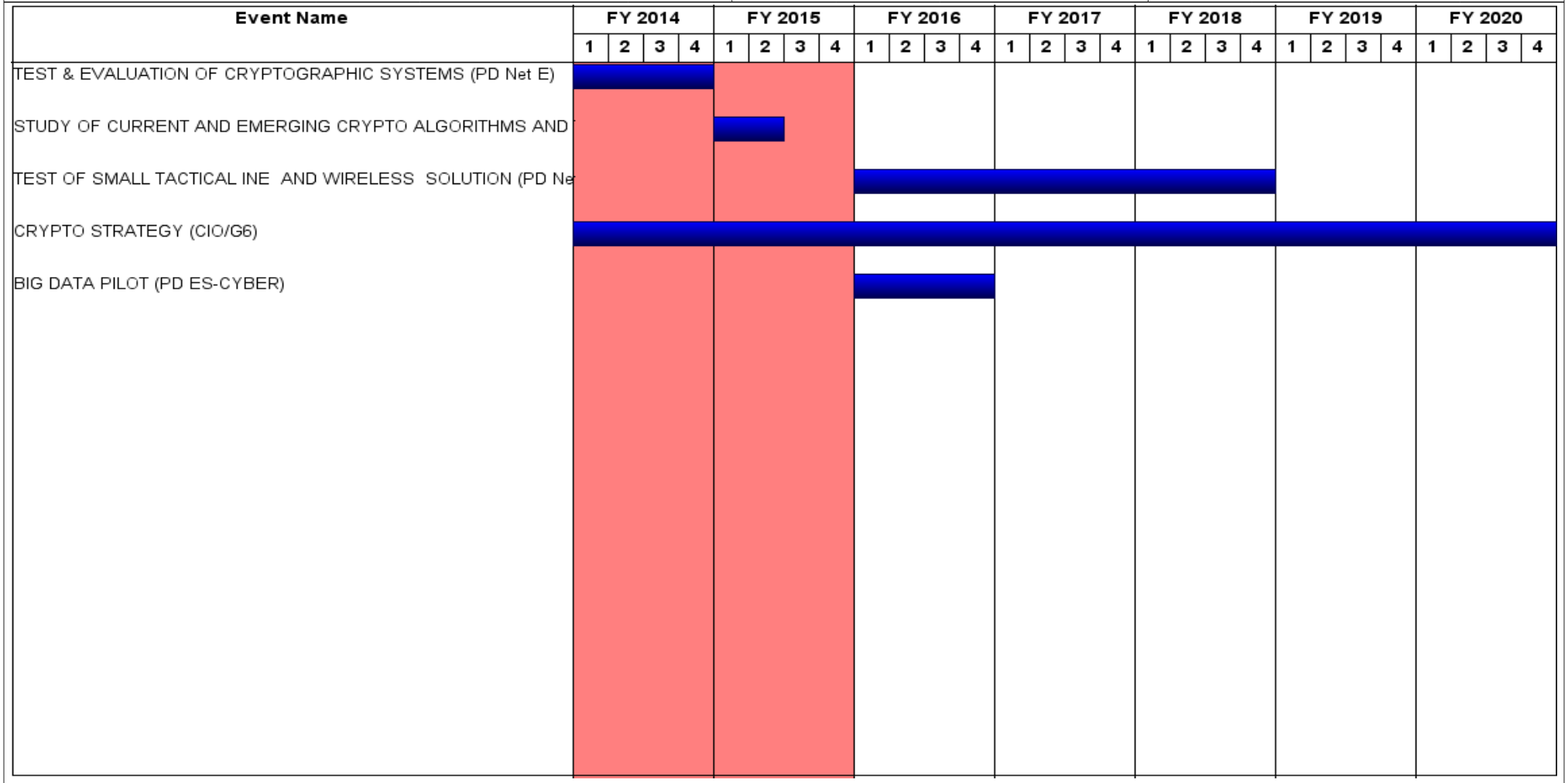

Exhibit R-4A, RDT&E Schedule Details: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
TEST & EVALUATION OF CRYPTOGRAPHIC SYSTEMS (PD Net E)	1	2014	4	2014
STUDY OF CURRENT AND EMERGING CRYPTO ALGORITHMS AND TECHNOLOGIES (PD Net E)	1	2015	2	2015
TEST OF SMALL TACTICAL INE AND WIRELESS SOLUTION (PD Net E)	1	2016	4	2018
CRYPTO STRATEGY (CIO/G6)	1	2014	4	2020
BIG DATA PILOT (PD ES-CYBER)	1	2016	4	2016

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army			Date: February 2015
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 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
501: *Army Key Mgt System*	-	1.262	1.183	1.927	-	1.927	2.328	2.568	-	-	-	9.268
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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) 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). 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).

MPMSS creates a secure, highly automated interface enabling transparent provisioning of KMI products. MPMSS capability is 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 MPMSS interface specification through FY17. The Army must then adjust to these changes delivered by NSA.

One major enhancement in the KMI architecture is the ability for OTNK. The end state for the Army is to make all 1.5 million legacy ECUs KMI aware with OTNK. Within AKMS this capability will be focused on the SKL. The 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 are expected to begin in FY2015 and continue throughout the POM.

To support this transition, a new KMI compliant cryptographic engine must be developed. The KOV-21 card used in current Army Tier 3 fill devices has hardware obsolescence issues and does not support OTNK. Redesigning and developmental efforts using modern and readily 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 2014	FY 2015	FY 2016
Title: Mission Planning Management Support System (MPMSS) Interface	1.262	1.183	1.021

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
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; Spins 1-4, through FY17. ***FY 2014 Accomplishments:*** The base capabilities for the MPMSS will be completed in the KMI Spiral 2 Spin 1 which was delivered in Aug 2014. This release will include the 1) migration to the addition of missing mission planning data fields based on the CERDEC evaluation of Sprint 9/ Release 1, 2) the initial Trusted Virtual Environment domain structure, and 3) the upgrade of Operating Systems. ***FY 2015 Plans:*** 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 ***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:***	-	-	0.906

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
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 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	1.262	1.183	1.927

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• BA1201: *TSEC - AKMS*	13.890	10.382	10.373	-	10.373	10.840	10.972	14.850	16.785	Continuing	Continuing
• B96004: *Key Management Infrastructure*	3.377	41.113	45.678	-	45.678	52.976	49.975	74.511	78.297	Continuing	Continuing
• DV4: *Key Management Infrastructure*	1.451	2.163	2.009	-	2.009	2.382	2.214	3.333	-	-	13.552

Remarks

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

D. Acquisition Strategy

Army Key Management System (AKMS) is an ACAT III Program of Record (POR) under PD Network Enablers (PD 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 2016 Army		Date: February 2015
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. PD 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 eoffort that began in FY14.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2016 Army			Date: February 2015
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 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MPMSS	MIPR	NSA : Linthicum, MD	2.250	0.557		-		-		-		-	Continuing	Continuing	Continuing
MPMSS Army Interface	MIPR	TBD : APG, MD	0.000	-		1.183		1.021		-		1.021	Continuing	Continuing	Continuing
KMI Awareness for Legacy Devices	C/CPFF	CERDEC S&TCD : APG, MD	0.000	-		-		0.906		-		0.906	Continuing	Continuing	Continuing
		Subtotal	2.250	0.557		1.183		1.927		-		1.927	-	-	-

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	2.186	0.353		-		-		-		-	-	2.539	-
		Subtotal	2.186	0.353		-		-		-		-	-	2.539	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	2.331	0.352		-		-		-		-	-	2.683	-
		Subtotal	2.331	0.352		-		-		-		-	-	2.683	-

	Prior Years	FY 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	6.767	1.262		1.183		1.927		-		1.927	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Army		Date: February 2015
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*

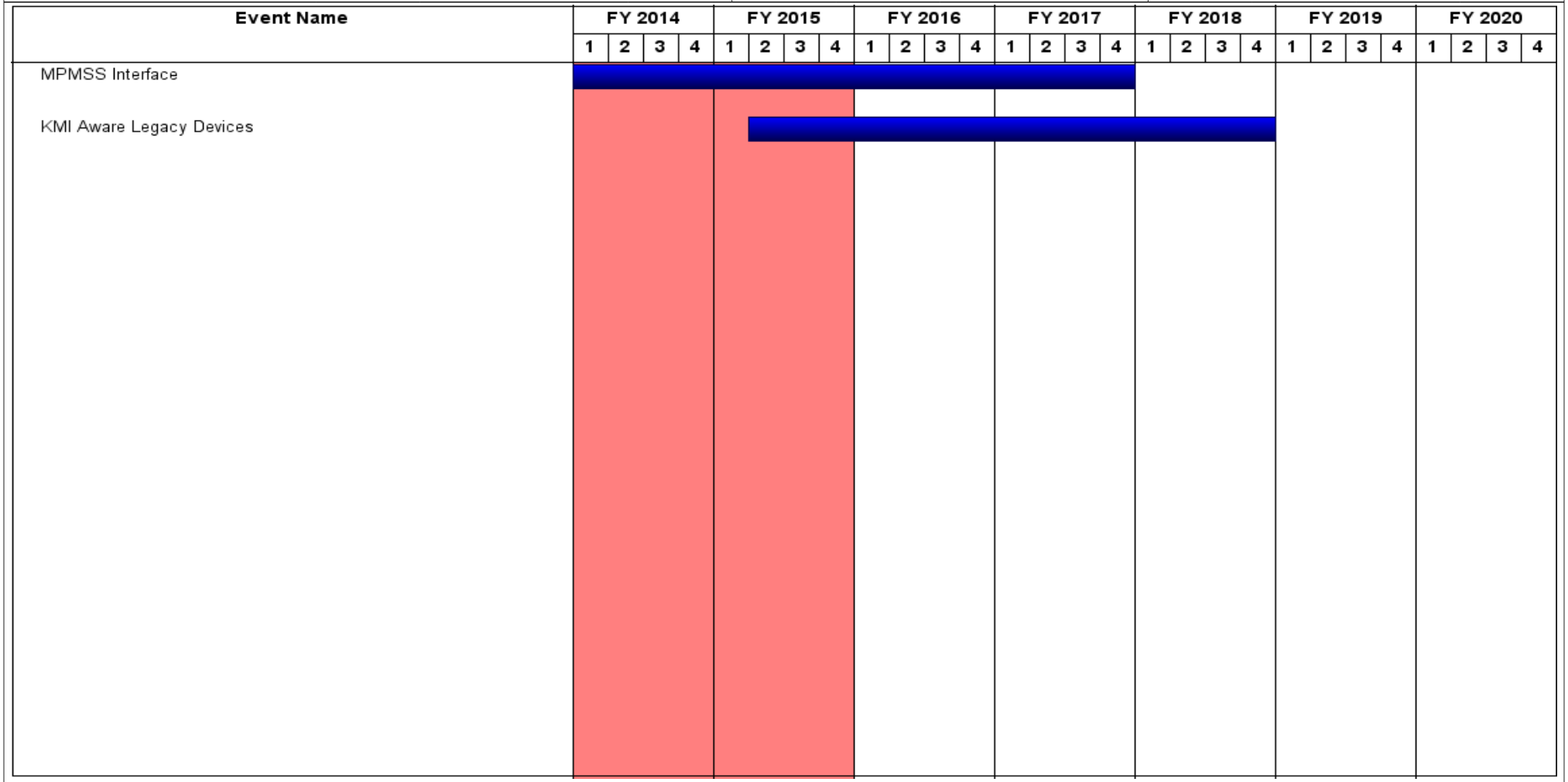

Exhibit R-4A, RDT&E Schedule Details: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
MPMSS Interface	1	2013	4	2017
KMI Aware Legacy Devices	2	2015	4	2018

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army											Date: February 2015	
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**Cost To Complete**	**Total Cost**
DV4: *Key Management Infrastructure (KMI)*	-	1.451	2.163	2.009	-	2.009	2.382	2.214	3.333	-	-	13.552
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Key management Infrastructure (KMI) (DV4) was realigned from project 491 in FY2014. KMI 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). KMI automates the functions of Communications Security (COMSEC) electronic key management, control, planning, and distribution. KMI 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 System of Systems (SoS) include the Management Clients (MGC), Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family. KMI provides an integrated, operational environment that brings essential key management personnel and functions in-band. AKMI achieves an Over the Network Keying (OTNK) solution to support emerging cryptographically modernized systems.

Two critical components required for the transition of AKMS to AKMI include the development of the Mission Planning Management Support System (MPMSS) and the ability to support OTNK.

MPMSS creates a secure, highly automated interface enabling transparent provisioning of KMI products. MPMSS capability is 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.

The developmental efforts for MPMSS are resourced in the 501 project line.

One major enhancement in the KMI architecture is the ability for OTNK. The end state for the Army is to make all 1.5 million legacy ECUs KMI aware with OTNK. The OTNK capabilities within the AKMI SoS will be found in the Next Generation Fill device family as outlined within the NGLD Capabilities Production Document. NGLD will be an enduring solution to bridge the gap until ~1.5 million legacy ECUs can be recognized on the KMI network or until they can be upgraded to be fully KMI aware.

The NGLD is reliant on a new KMI compliant cryptographic engine that must be developed. The KOV-21 card used in current Army Tier 3 fill devices has hardware obsolescence issues and does not support OTNK. Redesigning and developmental efforts using modern and readily available components for use in the Army's

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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)*

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 2014	FY 2015	FY 2016
Title: Key Management Infrastructure (KMI) Awareness (RESCUE / KOV-21 Replacement Effort)	-	2.163	2.009
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 KMI CPD that were technologically unachievable with the KOV 21 card. ***FY 2015 Plans:*** 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 (PD Net E). The RESCUE effort is focused on the development, maturation, evaluation, and certification of the technology needed to meet the requirements of the Army's NGLDs and can be reused, scaled, and/or repackaged to satisfy the requirements for legacy ECUs, enabling a KMI aware ECU fleet. The RESCUE effort will mature the required cryptographic technology to a Technology Readiness level (TRL) of six (acceptable) or seven (desired). Once the RESCUE reaches its desired TRL, it will be tailored for use as the cryptographic engine for the development of the KOV-21replacement card. 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 OTNK capability that can be inserted into the SKL to make it an NGLD Medium.			
Title: Key Management Infrastructure (KMI) Awareness	1.451	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
Description: KMI Awareness initiative creates a secure, highly automated interface in providing future OTNK capability to legacy 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. ***FY 2014 Accomplishments:*** Additional Mission Planning Management Support System (MPMSS) capabilities projected to be developed include 1) registration of MPMSS identities, 2) validations required for digital signature based on KMI and other medium assurance Public Key Infrastructure (PKI), 3) allowing the exchange of an electronic equivalent of a signed SF-153 (Hand Receipt, Destruction, Inventory, etc) and 4) integrating MP/MSS Application Program Interface (API) into the Army Mission Planner - Joint Tactical Network Environment NetOps Toolkit (JTNT).			
Accomplishments/Planned Programs Subtotals	1.451	2.163	2.009

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	3.377	41.113	45.678	-	45.678	52.976	49.975	74.511	78.297	Continuing	Continuing
• BA1201: *TSEC - Army Key Mgt Sys (AKMS)*	13.890	10.382	10.373	-	10.373	10.840	10.972	14.850	16.785	Continuing	Continuing
• 501: *Army Key Management System (AKMS)*	1.262	1.183	1.927	-	1.927	2.328	2.568	-	-	-	9.268

Remarks

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

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) is a Non Program of Record (POR) under PD Network Enablers (PD 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.

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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)*

AKMI initial Army Acquisition Program Baseline (APB) was approved 2QFY12. The AKMI System of Systems (SoS) will include the Management Clients (MGC), Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family. Each component of the AKMI SoS 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 SoS will be retained and adapted from the legacy AKMS program while others will be developed and fielded to meet AKMI requirements.

The MGC component of the AKMI SoS (AN/GYK-72(V)1) is currently being fielded. The MGC is assigned to the COMSEC Account Manager/COMSEC Custodian. MGC low rate initial production began in FY12 and full rate production was achieved in FY13. The Army has fielded Spiral 1 Spin 1 MGCs to 20 test and pilot accounts. The remaining Army accounts will be fielded Spiral 2 Spin 1 or Spiral 2 Spin 2 software version before the NSA mandated EKMS Tier 2 sunset of December 2017. MGC hardware will begin transition to CSLA for sustainment once all accounts are fielded.

The ACES component of the AKMI SoS (AN/GYK-33) hardware platform will be a non-ruggedized laptop fielded to S6, Spectrum Managers and some COMSEC Account Managers at Battalion level and above. ACES will be retained from the legacy AKMS program to support planning requirements and key distribution for KMI. Software will continued to be released on an annual basis to coincide with the Capability Set delivery schedule. As the Tier 2.5 component, ACES will operate between the MGC (Tier 2) and the NGLD (Tier 3). It links the key data from the MGC with mission planning data for a single load by the NGLD into the ECUs. ACES will require adaptations to meet AKMI requirements and incorporate capabilities provided by the AKMI SoS CONOPS.

The NGLD family will become the primary Army fill device and Tier 3 component of the AKMI SoS. 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 Army is evaluating existing fill devices to determine if they meet the NGLD small requirement. The Army will gain the NGLD medium capability through the SKL v3.1 in combination with a new KMI compliant cryptographic engine. The SKL v3.1 will be available in FY15. The AKMI program is partnering with RDECOM CERDEC to develop a KMI compliant cryptographic engine. The Army NGLD large strategy is highly reliant on the development of the new KMI compliant cryptographic engine and will drive a final acquisition decision in FY18.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2016 Army			Date: February 2015
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 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 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	-		2.163		2.009		-		2.009	Continuing	Continuing	Continuing
KMI Awareness	C/CPFF	CERDEC, S&TCD : APG, MD	0.000	1.451		-		-		-		-	Continuing	Continuing	Continuing
		Subtotal	0.000	1.451		2.163		2.009		-		2.009	-	-	-

	Prior Years	FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	1.451		2.163		2.009		-		2.009	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Army		Date: February 2015
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)*

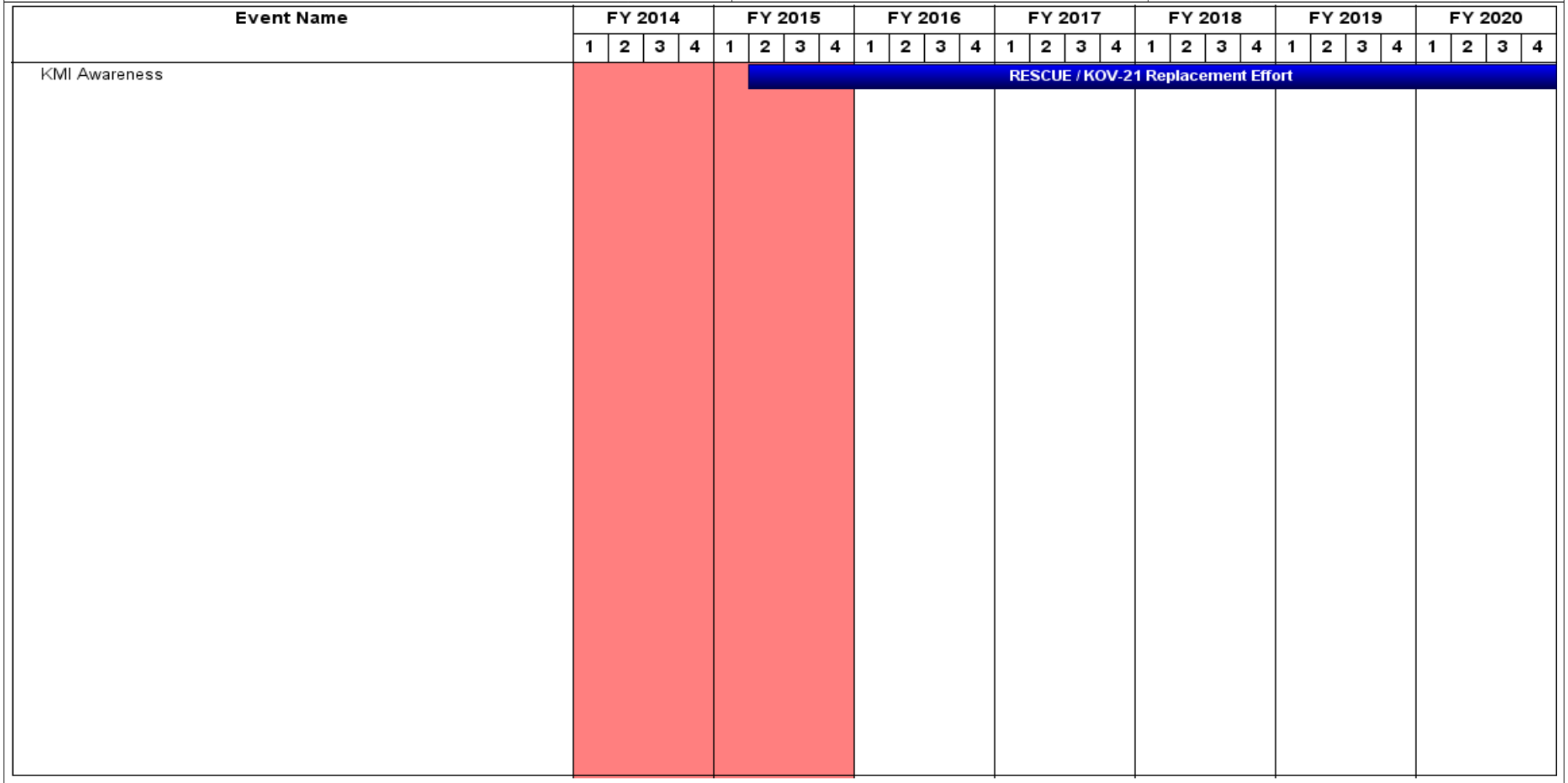

Exhibit R-4A, RDT&E Schedule Details: PB 2016 Army		Date: February 2015
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
KMI Awareness	2	2015	4	2020

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army											Date: February 2015	
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**Cost To Complete**	**Total Cost**
DV5: *Crypto Modernization (Crypto Mod)*	-	1.387	3.624	9.209	-	9.209	12.307	12.563	13.536	6.871	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 Cryptographic Modernization Initiative (CMI) is designed to investigate Courses Of Action (COAs), conduct a Material Solution Analysis (MSA), 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.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2014	FY 2015	FY 2016
Title: Crypto Solutions for Low Bandwidth Communications at the Tactical Edge	0.520	-	-
Description: This program creates tools that can be used with current and future methodologies in order to determine what amount of cryptographic solutions can be deployed at the tactical edge. This experimentation will allow for the WarFighter to have optimized solutions tailored for their specific program requirements while also showing trade-offs between competing solutions. Examples of common analysis to be performed are comparisons in encryption implementations, network initialization overhead, comparison of emerging Commercial Solutions for Classified architectures with COMSEC architectures, development of new network security and management protocols optimized for low-bandwidth environments and impact of emerging dynamic capabilities that evade or obstruct the adversary.			
FY 2014 Accomplishments:			

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
Develop software for use in NS-2 and/or OPNet environments to target specific comparisons in COMSEC diversity and also comparisons with Commercial Solutions for Classified architectures. Study existing network security and management protocols to identify areas of improvement and propose optimizations and new protocol designs. Identify optimal placement of network discovery servers and key management infrastructure. Investigate use of single packet authorization and propose improvements that make networks and hosts less detectable			
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program ***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 2014 Accomplishments:*** The program tests and evaluates developmental 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 2015 Plans:*** 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.	0.867	0.500	0.500
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 Plans:*** 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	-	3.124	3.179

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016
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 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 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.			
Title: Embedded Cryptographic Modernization Initialization ***Description:*** The Embedded Cryptographic Modernization Initiative conducts research and analyses to determine optimal algorithms and engineering approaches to modernizing various cryptographic sub-systems that are embedded within Army communications systems and data links. The analyses 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 analyses to determine optimal algorithms and engineering approaches to modernizing various embedded cryptographic sub-systems within Army communications systems and data links. The analyses 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.	-	-	5.530
Accomplishments/Planned Programs Subtotals	1.387	3.624	9.209

Exhibit R-2A, RDT&E Project Justification: PB 2016 Army		Date: February 2015
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 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	4.940	7.197	18.009	-	18.009	8.670	8.971	7.403	-	-	55.190
• TA0600: *Information System Security Program - ISSP*	13.245	-	-	-	-	-	-	-	-	-	13.245
• B96002: *Cryptographic Systems (Crypto Sys)*	4.334	18.151	16.206	-	16.206	33.006	59.781	48.658	64.961	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	-	3.521	2.530	-	2.530	2.574	2.656	3.197	4.956	Continuing	Continuing

Remarks

491 - Information Assurance Developement - RDTE funds - funding executed by PM and CIO/G6
TA0600 - Information System Security Program - OPA2 funds
B96002 - Cryptographic Systems - OPA2 funds
BS9716 - NON PEO-SPARES - OPA4 funds

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.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2016 Army			Date: February 2015
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 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CECOM RDEC : APG, MD	0.000	0.340		0.932		0.945		-		0.945	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	0.000	0.359		1.716		1.725		-		1.725	Continuing	Continuing	-
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.000	0.215		0.235		0.245		-		0.245	Continuing	Continuing	-
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	0.000	0.358		0.613		0.625		-		0.625	Continuing	Continuing	-
Information Assurance System Engineering Support	C/FFP	DSCI : Aberdeen, Maryland	0.000	0.115		0.128		0.139		-		0.139	Continuing	Continuing	-
Embedded Crypto Modernization Support	C/LH	TBD : TBD	0.000	-		-		5.530		-		5.530	Continuing	Continuing	-
		Subtotal	0.000	1.387		3.624		9.209		-		9.209	-	-	-

	Prior Years	FY 2014 Cost	FY 2014 Award Date	FY 2015 Cost	FY 2015 Award Date	FY 2016 Base Cost	FY 2016 Base Award Date	FY 2016 OCO Cost	FY 2016 OCO Award Date	FY 2016 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	1.387		3.624		9.209		-		9.209	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Army		Date: February 2015
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 2016 Army		Date: February 2015
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	2016
TEST AND EVALUATION OF LINK/TRUNK ENCRYPTORS SOFTWARE	4	2013	4	2019
TEST AND EVALUATION OF SECURE VOICE SOFTWARE AND HARDWARE	4	2013	4	2020
TEST AND EVALUATION OF PROPOSED EMBEDDED CRYPTOGRAPHIC SOLUTIONS	4	2015	4	2020
TEST AND EVALUATION OF IN-LINK NETWORK ENCRYPTORS SOFTWARE & HARDWARE	4	2013	4	2020