Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Army											Date: May 2017	
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*							
COST ($ in Millions)	**Prior Years**	**FY 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
Total Program Element	-	31.032	38.280	132.438	-	132.438	90.008	53.033	22.848	20.752	Continuing	Continuing
491: *Information Assurance Development*	-	18.401	7.431	10.194	-	10.194	8.872	9.303	9.884	7.600	Continuing	Continuing
501: *Army Key Mgt System*	-	1.851	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	1.851
DV4: *Key Management Infrastructure (KMI)*	-	1.930	4.699	4.696	-	4.696	3.261	2.930	3.319	3.415	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	8.850	21.565	27.047	-	27.047	25.847	24.843	8.599	8.666	Continuing	Continuing
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	0.000	4.585	88.949	-	88.949	51.057	14.974	0.000	0.000	0.000	159.565
FF8: *Unit Activity Monitoring (UAM)*	-	0.000	0.000	1.552	-	1.552	0.971	0.983	1.046	1.071	0.000	5.623

A. Mission Description and Budget Item Justification

Information Assurance Development supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies within the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms into specific systems in support of securing the Army Tactical and Enterprise Networks. This entails architecture studies, system integration and testing, developing installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates Cyber Security (CS)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan.

Information Assurance Development funding Implements and establishes functional and technical boundaries of cryptographic, key management and Information Assurance (IA) capabilities In Coordination With (ICW) the NSA, the Defense Information Systems Agency (DISA), and Joint Services, to secure National Security Systems (NSS), and National Security Information (NSI). Technical evaluations assess the security, operational effectiveness and network interoperability of advanced concept technologies to develop policies, standards, and fundamental building blocks for Army COMSEC capabilities that reduce the risk of future material solutions that could underperform and disrupt classified operations. Develop and publish the Cryptographic Modernization strategy to identify, standardize, and govern the insertion of CS capabilities to bridge operational gaps and support the Department of Defense (DoD) and NSA mandated requirements to enhance network capacity while providing for secure information exchange of voice, video, and data IAW the Army Network Campaign Plan. This will be accomplished by interoperability evaluation, standards testing, and CS , System of System Network Vulnerability Assessments (SoS NVA) for Army Capability Sets for CS/COMSEC capabilities that provide protections for tactical and fixed infrastructure post, camp, and station networks.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Army	Date: May 2017
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140A *I Information Systems Security Program*

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

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. 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 (MGC) Nodes 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 AKMI is the Army's implementation of the NSA KMI ACAT IAM program. AKMI supports DoD Global Information Grid (GIG) Net Centric and Cryptographic Modernization Initiatives (CMI) and supports emerging requirements transitioned from the AKMS. AKMI 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 Command, Control, Communications, Computers, Intelligence (C4I) systems. The AKMI Program includes the MGC nodes, 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 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 Army Tactical and Enterprise Network. This entails architecture studies, system integration and testing, developing installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates emerging CS/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp, and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Army	Date: May 2017
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 cryptographic algorithms and keys. Tactical radios using embedded cryptographic systems will no longer be able to communicate securely after cease key dates documented in the Chairman of the Joint Chiefs Staff instruction (CJCSI) 6510. In order to ensure Warfighters continue to have secured communications (i.e., encrypted data and voice), Army tactical radios are required to modernize their cryptographic capabilities by implementing modern algorithms. If cease key dates are not met, the Army will be forced to communicate at risk.

B. Program Change Summary ($ in Millions)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	31.154	38.280	70.554	-	70.554
Current President's Budget	31.032	38.280	132.438	-	132.438
Total Adjustments	-0.122	0.000	61.884	-	61.884
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-1.227	-			
• Adjustments to Budget Years	1.105	0.000	61.884	-	61.884

Change Summary Explanation

FY16 increase to project 491 supports Defensive Cyber Pilot efforts.

In FY18 the following net adjustments were made:
Crypto Modernization (DV5): Decrease of $1.390 million based on requirement adjustment.
Embedded Crypto Modernization (ET9): Increase of $61.693 million for embedded crypto modernization in Army radios.
Information Assurance (491): Increase of $.102 million based on requirement adjustment.
Key Management Infrastructure (DV4): Decrease of $.860 million based on requirement adjustment.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
491: *Information Assurance Development*	-	18.401	7.431	10.194	-	10.194	8.872	9.303	9.884	7.600	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 within the Army by providing COMSEC system capabilities through encryption, trusted software, or standard operating procedures; integrating these mechanisms into specified systems in support of securing the Army Tactical and Enterprise Network.

This entails architecture studies, system integration and testing, developing, installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates Cyber Security (CS)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camps and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization Strategy Plan.

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

Develop and publish the Cryptographic Modernization strategy to identify, standardize, and govern the insertion of IA capabilities that will bridge operational gaps and support the DoD and NSA mandated requirements to enhance network capacity while providing secure information exchange of voice, video, and data IAW the Army Network Campaign Plan. This will be accomplished by interoperability evaluation, standards testing, and CS System of System Network Vulnerability Assessments (SoS NVA) Army Capability Sets for CS/COMSEC capabilities that provide protections for the tactical and fixed infrastructure post, camps, and station networks.

The Defensive Cyberspace Operations (DCO) program provides initial capabilities that enable passive and active cyberspace defense operations to preserve friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Big Data Pilot provides an advanced analytics capability capable of ingesting structured, semi-structured, and unstructured data from multiple data sources (e.g., Joint Regional Security Stacks (JRSS), intrusion detection systems, intrusion prevention systems, network device log files, trouble tickets, firewalls, proxies, web and applications server log files, etc) and provides situational awareness of the cyberspace battlefield. It provides the computer network defense provider with a common analytic platform which informs and reduces risk associated with future material solutions and forms a blueprint for future Big Data Analytics. Big Data (analysis-of-all DoD Information Network sensor data) provides two optimized 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

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

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 2016	FY 2017	FY 2018
Title: Assessing emerging COMSEC hardware and software systems and products (PL Net E)	1.074	1.170	1.466
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 2016 Accomplishments:*** Conducted 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, Secure Voice (SV) and 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) ***FY 2018 Plans:*** As the Army implements new network technology, Secure Voice (SV) and In-line Network Encryption (INE) devices must continue to be identified and tested for effectiveness and suitability. Key areas of investigation include cyber security, interoperability, and standards compliance. (PL Net E)			
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 Accomplishments:*** 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 CS capabilities to ensure interoperability to maintain compliance with DoD, NSA, and Army policies and regulations. (CIO/G6)	7.602	6.261	8.728
Description: The program provides oversight and guidance for technical research and evaluation of Cryptographic Modernization (CM) and Key Management (KM) capabilities to ensure IA compliance and interoperability. This effort improves operational			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018
effectiveness, ensures efficient implementation, and enhances network performance by deploying standardized COMSEC capabilities that are interoperable and supportable in Army, coalition and Joint operating environments. This program enables the Army to collaborate and participate in Joint and Army Capability Technology Demonstrations to define, improve, develop and publish Cyber Security (CS) standards for new/modernized technology insertion to support the LWN 2025 and Beyond. This effort assesses and defines risk mitigation of CS network vulnerabilities in end-to-end Army network operations and Common Operating Environment. (CIO/G6) ***FY 2016 Accomplishments:*** In support of Army and Combatant Commands world-wide, provided risk reduction lab tests to evaluate the maturity and security of new emerging technology which included trusted cyber sensor, Commercial Solutions for Classified (CSfC) and Cryptographic High Value Product (CHVP) Radio for unattended use to bridge operational gaps to enable secure communications between the tactical edge and DoD enterprise, and to align with the Army Network Campaign Plan and the DoD Joint Information Environment (JIE). Reviewed and assessed operational needs, standardized software testing, recommended software releases and identified fundamental building blocks for Cyber solutions. Provided policies and guidance for COMSEC programs and initiatives to ensure capabilities, interoperability, suitability remains synchronized with Army requirements. Provided security standards and technical input to the Army COMSEC Modernization Strategy. Developed Army cryptographic technology roadmaps to integrate modern technology and to assist Army organizations with phasing out legacy Crypto components. Participated in the NSA, DoD CIO, Joint Staff and Army forums to identify baseline requirements for the next generation of Cryptographic devices and future applications. Identified and submitted new Army security standards, performance and interoperability requirements for the upcoming NSA CryptoMod 2 Initial Capabilities Document (ICD) development. Identified and recommended changes to Army Technical Bulletins, Army Regulations and NSA CNSS Instructions. (CIO/G-6) ***FY 2017 Plans:*** Oversight and Implementation guidance that provides a framework for Army CM and KM 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 and to participate in joint tests with NSA, DISA, and Services to establish functional and technical boundaries for CM, KM, and CS operations. Collaborate with the NSA, DoD and Joint Staff to define new Advanced Cryptographic Capability (ACC) standards (security and interoperability) for the tactical and operational environment. The program resources CS System of Systems Network Vulnerability Assessments (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. ***FY 2018 Plans:*** Oversee execution of the Army's COMSEC Modernization initiative by identifying and developing new security baseline for implementation of Army CM and KM initiatives. Assess, review and validate Army operational needs. Test and evaluate CM			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018
and KM technologies to determine the maturity and viability for Army use to protect and strengthen the Network posture. Identify fundamental building blocks for IA solutions, perform risk reduction testing of commercial products prior to insertion into Army for use to increase operational availability with documented operational value and rapid integration. Collaborate with the NSA, DoD and Joint Staff to define new ACC standards (security and interoperability) for the tactical and operational environment. Provide continuous test and evaluate results to enable the Army to make sound investment strategic decisions and to reduce or eliminate duplications. Participate in operational assessment of NSA, DoD, Joint Staff and Service led Joint Capability Technology Demonstrations to align new technologies to documented Army and Service capability gaps for protecting National Security Systems and National Information. Develop strategies and policies that leverage emerging cryptographic and key management tools and services. (CIO/G6)			
Accomplishments/Planned Programs Subtotals	18.401	7.431	10.194

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• DV5: *Crypto Modernization*	8.850	21.565	27.047	-	27.047	25.847	24.843	8.599	8.666	Continuing	Continuing
• ET9: *Embedded Crypto Modernization*	-	4.585	88.949	-	88.949	51.057	14.974	-	-	0	159.565
• B96002: *Cryptographic Systems*	16.206	66.692	49.441	-	49.441	40.276	86.306	98.519	102.302	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	3.014	-	-	-	-	97.969	157.904	48.382	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	0.170	2.545	2.635	-	2.635	3.170	4.917	4.961	5.000	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.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Army		Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering (PL Net E)	SS/LH	CECOM RDEC : CECOM RDEC APG, MD	78.116	1.031		1.170		1.466		-		1.466	0.000	81.783	0.000
Big Data Pilot (PL ES-CYBER)	TBD	TBD : FT BELVOIR, VA	0.000	9.725		-		-		-		-	0.000	9.725	0.000
Information Assurance System Engineering Support (PL Net E)	C/FFP	DSCI Consulting : APG, MD	7.106	-		-		-		-		-	0.000	7.106	0.000
Engineering Support (PL Net E)	C/CPFF	CACI : APG, MD	5.018	-		-		-		-		-	0.000	5.018	0.000
Engineering Support (PL Net E)	C/CPFF	Booz Allen Hamilton : APG, MD	3.408	-		-		-		-		-	0.000	3.408	0.000
Engineering Support (PL Net E)	C/FP	CSC : APG, MD	16.448	-		-		-		-		-	0.000	16.448	0.000
Engineering Support (CIO/G6)	C/FP	CACI : APG, MD	3.879	1.245		1.595		2.196		-		2.196	Continuing	Continuing	Continuing
System Engineering (CIO/G6)	SS/LH	CECOM RDEC : APG, MD	1.698	2.073		1.086		1.496		-		1.496	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/CPFF	Booz Allen Hamilton : APG, MD	4.563	1.625		1.261		1.737		-		1.737	Continuing	Continuing	Continuing
Engineering Support (CIO/G6)	C/FFP	AASKI : Edgewood, MD	1.032	1.079		1.316		1.813		-		1.813	Continuing	Continuing	Continuing
Service (CIO/G6)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	3.346	1.623		1.003		1.486		-		1.486	Continuing	Continuing	Continuing
		Subtotal	124.614	18.401		7.431		10.194		-		10.194	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support (PL Net E)	C/CPFF	TBD : TBD	1.598	-		-		-		-		-	0	1.598	0

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Army			Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 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 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	126.212	18.401		7.431		10.194		-		10.194	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

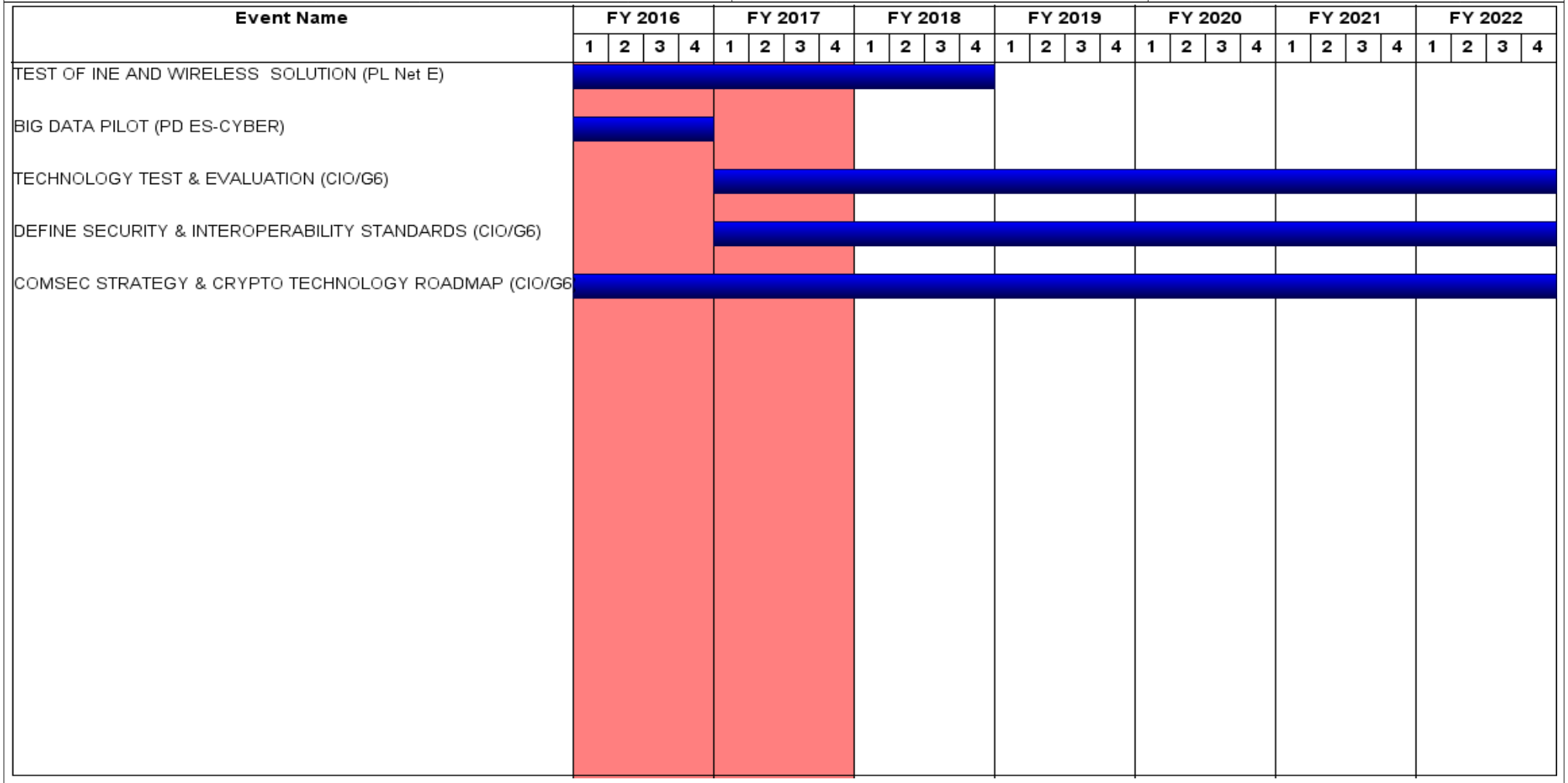

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
TEST OF INE AND WIRELESS SOLUTION (PL Net E)	1	2016	4	2018
BIG DATA PILOT (PD ES-CYBER)	1	2016	4	2016
TECHNOLOGY TEST & EVALUATION (CIO/G6)	1	2017	4	2022
DEFINE SECURITY & INTEROPERABILITY STANDARDS (CIO/G6)	1	2017	4	2022
COMSEC STRATEGY & CRYPTO TECHNOLOGY ROADMAP (CIO/G6)	1	2014	4	2022

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army				Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
501: *Army Key Mgt System*	-	1.851	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	1.851
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 (MGC) nodes 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: FY 2018 Army		Date: May 2017
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. AKMS RDT&E funding line 501 realigned to DV4 / KMI FY17 and out.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Mission Planning Management Support System (MPMSS) Interface	0.945	-	-
Description: The 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. National Security Agency (NSA) plans to deliver the MPMSS capabilities in 4 releases; Spirals 1-4, through FY16. ***FY 2016 Accomplishments:*** 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 End Crypto Units (ECU)s. 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 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 Accomplishments:*** 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	1.851	-	-

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• BA1201: *TSEC - AKMS*	10.373	-	-	-	-	-	-	-	-	0	10.373

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	45.678	63.578	58.363	-	58.363	59.875	65.784	55.349	73.765	Continuing	Continuing
• DV4: *Key Management Infrastructure*	1.930	4.699	4.696	-	4.696	3.261	2.930	3.319	3.415	Continuing	Continuing
• 432140: *ISSP (TSEC-AKMS) OMA*	7.380	8.006	8.316	-	8.316	8.678	3.945	4.043	4.119	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 ~1.5M 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.

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.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 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.

AKMS RDT&E funding line 501 realigned to DV4 / KMI FY17 and out.

E. Performance Metrics

N/A

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
DV4: *Key Management Infrastructure (KMI)*	-	1.930	4.699	4.696	-	4.696	3.261	2.930	3.319	3.415	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

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

A. Mission Description and Budget Item Justification

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

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

One of the major enhancement in the AKMI architecture is the ability 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 current KOV-21 card is referred to as the KOV-21 Replacement and is an extension of the RESCUE program as a technology insertion. The NGLD-Large

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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)*

technology development will start in FY2019. The NGLD-Large development will provide the same capabilities as the NGLD-Medium, along with wireless (802.11) and additional memory (64 GB) requirements.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Key Management Infrastructure (KMI) Awareness (RESCUE / KOV-21 Replacement Effort)	1.930	4.699	4.696
Description: KMI Awareness initiative creates a secure, highly automated interface in providing future Over the Network Keying (OTNK) capability to legacy End Crypto Units (ECU)s. This initiative will allow ECUs to receive, authenticate, and decrypt OTNK messages and increases WarFighter survivability by minimizing the need for Soldiers to travel to obtain keys. The KOV 21 card, previously in production through NSA for use in the Simple Key Loader (SKL) and the Secure DTD 2000 System (SDS), is nearing the end of life due to unavailability of parts. Redesigning and developmental efforts using modern and readily available components for use in the Army's SKL and Next Generation Load Devices (NGLDs) are currently underway. The redesign of the current KOV 21 card is referred to as the KOV 21 Replacement and is an extension of the KOV 21 card as a technology insertion. The KOV 21 Replacement will also address requirements codified in the NGLD CPD and the AKMI CPD that were technologically unachievable with the KOV 21 card. ***FY 2016 Accomplishments:*** The RESCUE technology development will continue in FY2017. RESCUE development will provide the ability to upgrade legacy fill devices, enabling a KMI aware fully developed PDE-enabled NGLD family of devices. The RESCUE effort lays the foundation for AKMI capabilities that can be integrated into the SKL v3.1 to make it an NGLD Medium. ***FY 2017 Plans:*** The RESCUE technology development will continue 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. ***FY 2018 Plans:*** The RESCUE technology development will complete in FY2018. RESCUE development will provide the ability to upgrade legacy ECUs, enabling a KMI aware fully developed PDE-enabled ECU fleet. The KOV-21 Replacement effort lays the foundation for AKMI capabilities that can be inserted into the SKL to make it an NGLD Medium.			
Accomplishments/Planned Programs Subtotals	1.930	4.699	4.696

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	45.678	63.578	58.363	-	58.363	59.875	65.784	55.349	73.765	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• BA1201: *TSEC - Army Key Mgt Sys (AKMS)*	10.373	-	-	-	-	-	-	-	-	0	10.373
• 501: *Army Key Management System (AKMS)*	1.851	-	-	-	-	-	-	-	-	0	1.851
• 432140: *ISSP (TSEC-AKMS)*	7.385	8.006	8.316	-	8.316	8.678	3.945	4.043	4.119	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 Project Lead Network Enablers (PL Net E). AKMI is the Army's implementation of the National Security Agency (NSA) Key Management Infrastructure (KMI) ACAT IAM Program of Record. The AKMI will allow the Army to manage, control, plan, and distribute electronic key for the ~1.5M End Cryptographic Units (ECU)s necessary to communicate and distribute data on the Army's tactical and strategic networks.

AKMI initial Army Acquisition Program Baseline (APB) was approved 2QFY12. The AKMI Program will include the Management Clients (MGC) nodes, Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD) Family. Each component of the AKMI Program is in a different phase of the acquisition cycle.

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

The NGLD family of devices will become the primary Army fill devices and Tier 3 component of the AKMI Program. The NGLD Capability Production Document (CPD) was signed 4QFY13. The NGLD CPD calls for a family of 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 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

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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)*

requirements. The NGLD Medium will be available in FY19. Additionally, the Army NGLD large strategy is highly reliant on the development of the RESCUE and will drive a materiel solution decision in FY19.

E. Performance Metrics

N/A

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	8.850	21.565	27.047	-	27.047	25.847	24.843	8.599	8.666	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 Army Tactical and Enterprise Networks.

This entails architecture studies, system integration and testing, developing installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates emerging Information Assurance (IA)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp, and station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan.

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program	0.500	0.500	0.500
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 2016 Accomplishments:			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018
The program tested and evaluated engineering changes to Low Rate Initial Production (LRIP) of VACM devices to confirm continued capability and interoperability on Army networks and tactical systems and identified new risk areas for compliance with COMSEC regulations and procedures. ***FY 2017 Plans:*** The program will continue to test and evaluate engineering changes to Full Rate Production (FRP) of VACM devices to confirm continued capability and interoperability on Army networks and tactical systems as well as identifying new risk areas for compliance with COMSEC regulations and procedures. ***FY 2018 Plans:*** The program will continue to test and evaluate engineering changes to Full Rate Production (FRP) of VACM devices to confirm continued capability and interoperability on Army networks and tactical systems as well as identifying new risk areas for compliance with COMSEC regulations and procedures. Will begin fielding to Secret level users performing site surveys and installing at both CONUS and OCONUS locations.			
Title: Cryptographic Systems Test and Evaluation ***Description:*** This program supports the Army Cryptographic Modernization Transformational Initiative. This is accomplished by providing test and evaluation capabilities to the COMSEC community in order to assess emerging technologies before being released and approved for Army use; testing will be performed on hardware, software and network systems. ***FY 2016 Accomplishments:*** The program tested and evaluated of COMSEC devices to confirm capability and interoperability on Army networks and tactical systems and identified risk areas for compliance with COMSEC regulations and procedures. The program tested and evaluated 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 High Assurance Internet Protocol Encryptor (HAIPE) 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. The program tested interfaces and provided ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluated performance of technologies and provided direction to ensure 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	3.120	4.314	5.450

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018
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 to ensure 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. ***FY 2018 Plans:*** The program continues testing and evaluation of COMSEC devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, CHVP, CSfC Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. The program tests interfaces and provides ways to insert DAR and DIT technology within the existing and future network infrastructure. Evaluates performance of technologies and provides direction to ensure the lowest impact on performance while providing the greatest protection from loss of sensitive data.			
Title: High Assurance Internet Protocol Encryption (HAIPE) extension manager ***Description:*** A management tool to configure the new extensions to the HAIPE standard and process the resulting data to provide early indications of cyber attacks. ***FY 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. ***FY 2018 Plans:*** Continue a software development efforts that will provide configuration and management of the HAIPE extensions and the user interface for collecting and analyzing the data that results from implementation of these HAIPE extensions. This will facilitate the upgrade of the Army HAIPEs to include new cyber-sensor functionality for the tactical cyber cell.	-	1.503	1.748
Title: Embedded Cryptographic Modernization Initiative (ECMI) ***Description:*** The ECMI is an upgrade activity that will ensure enduring Army radios remain secure by operating with modern cryptographic algorithms and keys. Funding secured in DV5 line to support ECMI Non Recurring Engineering (NRE) efforts to comply with cease key dates mandated by CJCSI 6510. ***FY 2016 Accomplishments:***	5.230	15.248	19.349

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018
Determined optimal algorithms and engineering approaches to modernize various embedded cryptographic modules within Army communications systems and data links. The analysis and resulting program plans used a complete life cycle approach and included fielding, training, and sustainment as well as the technical approach to ensure compliance with NSA mandated cease key dates, while minimizing cost. Initiated contract for, the necessary non-recurring testing, engineering and development of hardware and software. Preliminary fielding and training plans developed. ***FY 2017 Plans:*** Software engineering and coding to upgrade the government purpose rights software code used in software defined radios to ensure these radios remain secure by employing algorithms and keys that comply with CJCSI 6510. System engineering activities including detailed requirements decomposition, and functional allocation. Design of modern reprogrammable cryptographic modules. Detailed hardware design and software coding. ***FY 2018 Plans:*** Continue execution of NRE efforts to develop, design, test/evaluate, and certify cryptographic hardware and software embedded in tactical radios to ensure these radios remain secure. System engineering activities including detailed requirements decomposition, and functional allocation. Design of modern reprogrammable cryptographic modules. Detailed hardware design and software coding.			
Accomplishments/Planned Programs Subtotals	8.850	21.565	27.047

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	18.401	7.431	10.194	-	10.194	8.872	9.303	9.884	7.600	Continuing	Continuing
• ET9: *Embedded Crypto Modernization*	-	4.585	88.949	-	88.949	51.057	14.974	-	-	0.000	159.565
• B96002: *Cryptographic Systems*	16.206	66.692	49.441	-	49.441	40.276	86.306	98.519	102.302	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	3.014	-	-	-	-	97.969	157.904	48.382	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	0.170	2.545	2.635	-	2.635	3.170	4.917	4.961	5.000	Continuing	Continuing

Remarks

Line Item & Title:
491 - Information Assurance Development - RDTE - funding executed by PL Net E, CIO/G6 and PL ES-CYBER
ET9 - Embedded Crypto Modernization - RDTE

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
B96002 - Cryptographic Systems - OPA2											
B96006 - Embedded Cryptographic Modernization - OPA2											
BS9716 - NON PEO-SPARES - OPA4											

D. Acquisition Strategy

The objective of this program is to integrate and validate hardware and software solutions to provide COMSEC superiority in order to protect against threats, increase battlefield survivability/lethality, and enable critical Mission Command activities. The objective of the Cryptographic Systems program is to provide adaptive, flexible, and programmable cryptographic systems using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic systems. The effort will support the network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating networked vulnerabilities to Army information security systems. CDD, approved by CIO/G6, 15 Jul 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: FY 2018 Army			Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	SS/LH	CECOM RDEC : APG, MD	1.272	0.965		1.682		2.133		-		2.133	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	1.937	1.646		1.515		1.600		-		1.600	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.450	0.245		1.725		1.953		-		1.953	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	0.971	0.625		1.148		1.757		-		1.757	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/FFP	DSCI : Aberdeen, Maryland	0.243	0.139		0.247		0.255		-		0.255	Continuing	Continuing	Continuing
Embedded Crypto Modernization Support	C/LH	TBD : TBD	0.000	5.230		15.248		19.349		-		19.349	Continuing	Continuing	Continuing
		Subtotal	4.873	8.850		21.565		27.047		-		27.047	-	-	-

	Prior Years	FY 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	4.873	8.850		21.565		27.047		-		27.047	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Army		Date: May 2017
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)*

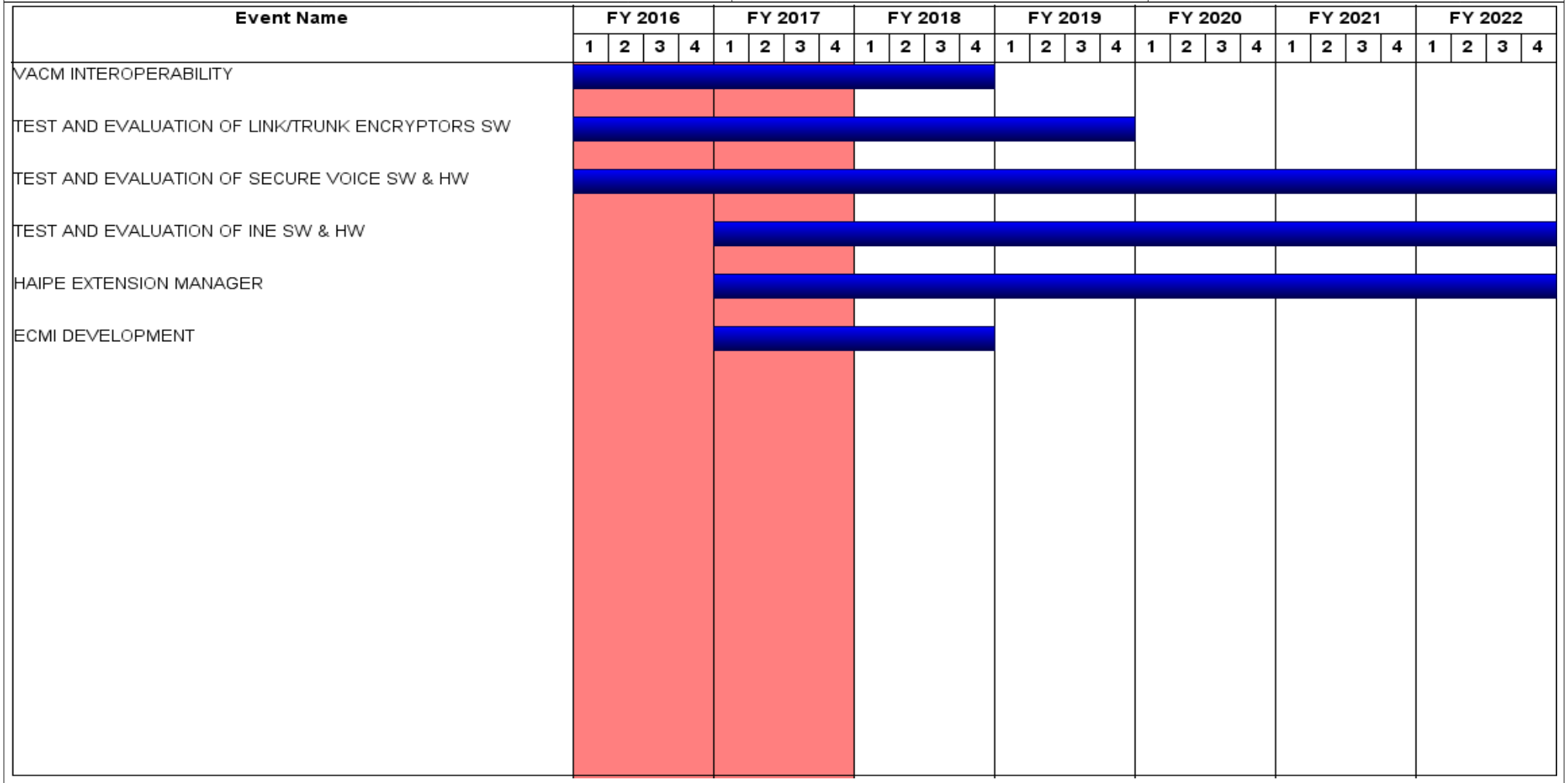

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

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

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
ET9: *Embedded Crypto Modernization (CRYPTO MOD)*	-	0.000	4.585	88.949	-	88.949	51.057	14.974	0.000	0.000	0.000	159.565
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

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

A. Mission Description and Budget Item Justification

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Embedded Cryptographic Modernization Initiative (ECMI) Development Contracts	-	4.585	88.949
Description: ECMI Non Recurring Engineering (NRE) Contract Prep Work and Execution ***FY 2017 Plans:*** Complete acquisition documentation and award contracts to develop, design, test/evaluate, and certify cryptographic hardware and software embedded in tactical radios to ensure these radios remain secure. System engineering activities including detailed requirements decomposition, and functional allocation. Design of modern reprogrammable cryptographic modules. Detailed hardware design and software coding. ***FY 2018 Plans:*** Support NRE development of ECMI efforts for vendor developmental and production contracts which supports NSA mandated Cease Key Date IAW CJCSI 6510.02E. This capability will ensure Army tactical radios possess the latest cryptographic solutions.			
Accomplishments/Planned Programs Subtotals	-	4.585	88.949

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	18.401	7.431	10.194	-	10.194	8.872	9.303	9.884	7.600	Continuing	Continuing
• DV5: *Crypto Modernization*	8.850	21.565	27.047	-	27.047	25.847	24.843	8.599	8.666	Continuing	Continuing
• B96002: *Cryptographic Systems*	16.206	66.692	49.441	-	49.441	40.276	86.306	98.519	102.302	Continuing	Continuing
• B96006: *Embedded Cryptographic Modernization*	-	3.014	-	-	-	-	97.969	157.904	48.382	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	0.170	2.545	2.635	-	2.635	3.170	4.917	4.961	5.000	Continuing	Continuing

Remarks

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

D. Acquisition Strategy

The objective of the 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: FY 2018 Army			Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
PL NET E Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	0.000	-		2.837		4.968		-		4.968	Continuing	Continuing	Continuing
PM TR Program Mgmt Personnel	C/CPFF	BAH : Aberdeen, MD	0.000	-		1.424		-		-		-	Continuing	Continuing	Continuing
PM TR Program Mgmt Personnel	C/CPFF	TBD : Aberdeen, MD	0.000	-		0.324		-		-		-	Continuing	Continuing	Continuing
ECMI Development Contracts	C/CPFF	TBD : TBD	0.000	-		-		83.981		-		83.981	Continuing	Continuing	Continuing
		Subtotal	0.000	-		4.585		88.949		-		88.949	-	-	-

	Prior Years	FY 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	-		4.585		88.949		-		88.949	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Army		Date: May 2017
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)*

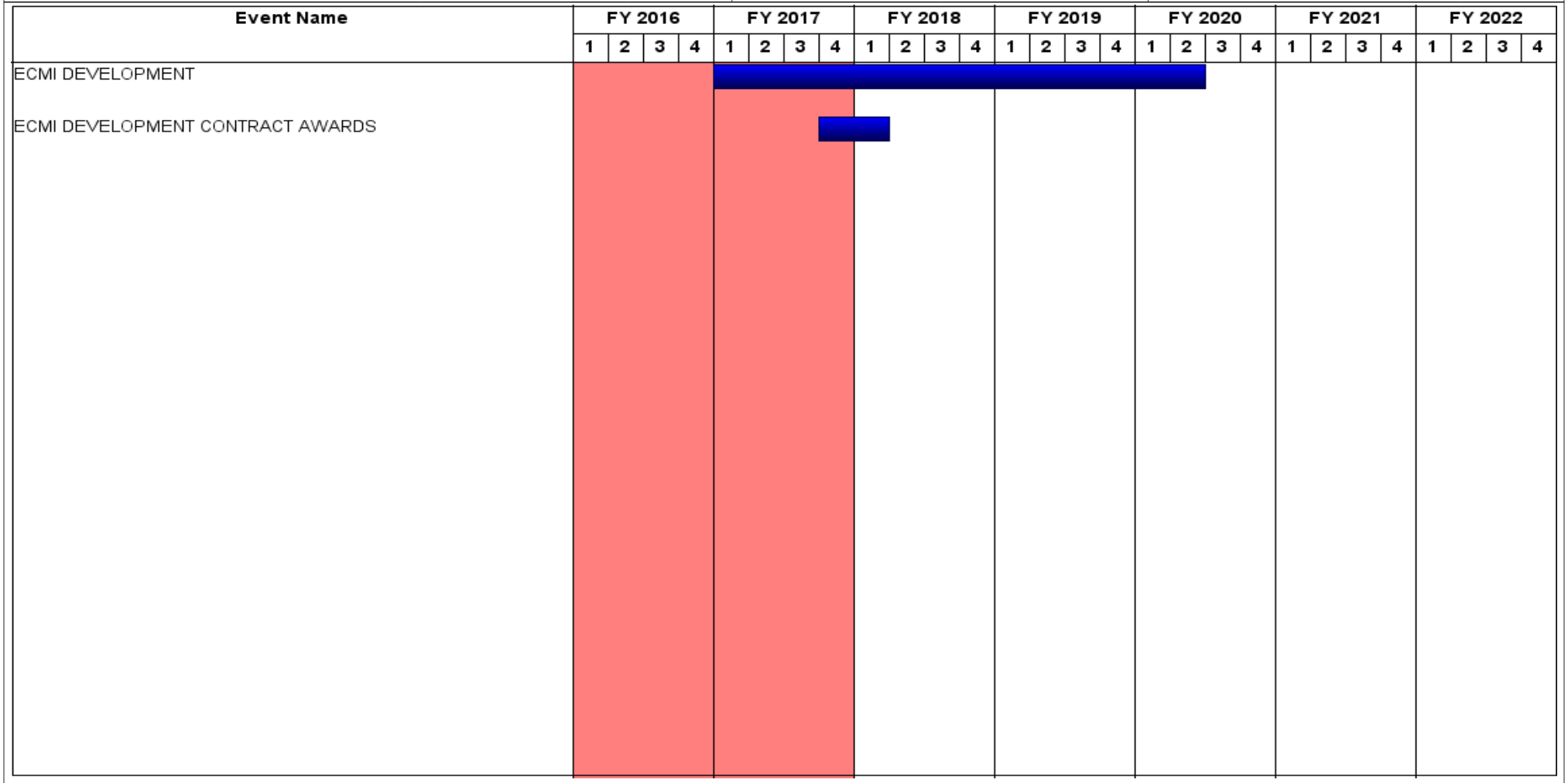

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** ET9 / *Embedded Crypto Modernization (CRYPTO MOD)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
ECMI DEVELOPMENT	1	2017	2	2020
ECMI DEVELOPMENT CONTRACT AWARDS	4	2017	1	2018

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army			Date: May 2017
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) FF8 / *Unit Activity Monitoring (UAM)*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
FF8: *Unit Activity Monitoring (UAM)*	-	0.000	0.000	1.552	-	1.552	0.971	0.983	1.046	1.071	0.000	5.623
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

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

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Unit Activity Monitoring	-	-	1.552
Description: FY 2018 marks the first UAM automation/analytics program year. FY 2018 Base funds in the total amount of $1.552 million are provided for software engineering development and testing resources to enhance the Army' UAM data processing, analysis, and data visualization capabilities, and its workflow management system, plus the integration of new data sources into the data processing component. All work is focused on the development of new capabilities. The details of this program are reported in accordance with Title 10, United States Code, Section 119(a)(1). ***FY 2018 Plans:*** Unit Activity Monitoring			
Accomplishments/Planned Programs Subtotals	-	-	1.552

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: FY 2018 Army		Date: May 2017
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** FF8 / *Unit Activity Monitoring (UAM)*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

FY18: The planned acquisition strategy to acquire UAM Automation/Analytics software engineering services is to award through the use of competitive acquisition, a Base plus three-option year firm-fixed price contract.

FY19: The planned acquisition is to exercise option year one of the software engineering services contract.

E. Performance Metrics

N/A