

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>
--	--

COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
Total Program Element	123.348	91.657	69.133	-	69.133	85.696	72.941	81.125	86.124	Continuing	Continuing
674861: <i>EKMS (Electronic Key Management System)</i>	4.086	1.777	2.033	-	2.033	2.059	0.603	0.647	0.950	Continuing	Continuing
675100: <i>Cryptographic Modernization</i>	103.145	67.387	51.086	-	51.086	67.233	56.841	63.888	68.032	Continuing	Continuing
675231: <i>AF Key Management Infrastructure (AF KMI)</i>	6.352	16.471	10.342	-	10.342	10.551	9.536	10.409	10.852	Continuing	Continuing
677820: <i>Computer Security RDT&E: Firestarter</i>	9.765	6.022	5.672	-	5.672	5.853	5.961	6.181	6.290	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information Systems Security Program Element provides cradle-to-grave research, development, acquisitions, supply, sustainment, depot maintenance and demilitarization of the Air Force (AF) cryptographic and key distribution/management systems. Additionally, it funds the AF operation one of two US National Security Agency Tier 1 key distribution centers, the AF Public Key Infrastructure System Program Office, the AF Call Sign function, and a special computer security program designated, Firestarter.

The overall focus of the Research, Development, Test, and Evaluation (RDT&E) efforts within this program is two-fold. The major focus is transforming electronic key delivery and DoD cryptographic devices to meet the next generation warfighting requirements. This focus is driven by the National Security Agency's tenets calling for (1) a totally "man-out-of-the-loop" electronic crypto key distribution system from the actual generation of the key in the key processor all the way into the using End Crypto Unit (ECU) (eliminates the current key vulnerability to compromise by individuals transporting or loading the key); and (2) an inventory of cryptographic devices that are more robust, modular, scalable, capable, net-centric, and durable (allows more effective and efficient performance including reduced inventory, expanded data rates, simplified upgrades, and ensured global information grid-compatibility). The second focus is to rapidly provide new/improved capabilities to 24 AF-led forces further enabling them to protect and defend USAF Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) and Weapon Systems from Information Warfare (IW) attacks and to ensure affected system recovery from such attacks. To this end, the project does research and development of information protection tools and transitions them to operational systems. These efforts not only provide AF passive Net Defense capabilities but also an increasing share of the active Net Defense capabilities.

This program is in Budget Activity 7, Operational System Development, these budget activities include development efforts to upgrade systems currently fielded or has approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>
--	--

B. Program Change Summary (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Previous President's Budget	140.017	101.788	82.372	-	82.372
Current President's Budget	123.348	91.657	69.133	-	69.133
Total Adjustments	-16.669	-10.131	-13.239	-	-13.239
• Congressional General Reductions	-	-1.131			
• Congressional Directed Reductions	-	-9.000			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-10.000	-			
• SBIR/STTR Transfer	-4.893	-			
• Other Adjustments	-1.776	-	-13.239	-	-13.239

Change Summary Explanation

FY11 Congressional General Reduction of 1.776M in Other Adjustment row.

FY12 Congressional General Reduction (FFRDC, Sec. 8023) of 1.131M.

FY12 Congressional Directed Reduction of 9M due to Vinson/ANDVT Cryptographic Modernization (VACM) protest delay

FY13 funding decrease is due to higher Department of Defense priorities.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 674861: <i>EKMS (Electronic Key Management System)</i>
--	--	--

COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
674861: <i>EKMS (Electronic Key Management System)</i>	4.086	1.777	2.033	-	2.033	2.059	0.603	0.647	0.950	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Air Force Electronic Key Management System (AFEKMS) Program consists of multiple developments supporting the Air Force requirements portion of the DoD EKMS Program. (The National Security Agency [NSA] acts as the Executive Agency for the DoD EKMS Program.) AFEKMS, in concert with the overarching DoD EKMS program, provides a secure and flexible capability for the electronic generation, distribution, accounting, and management of key material, voice callwords, and communications security (COMSEC) publications for the current generation of DoD Command, Control, Communications, Computers, and Intelligence (C4I) and for current generation of weapon systems. DoD EKMS replaced the previous manual distribution and management system providing cryptographic keying material for U.S. DoD Information Assurance. Information Assurance emphasizes confidentiality, access control, multi-level secure databases, trusted computing and information integrity. DoD EKMS has a three-tier hierarchical structure. This tiered structure provides capability to distribute, manage and account for COMSEC keying material. Tier 1 installations comprise the key material general and control capability. Tier 2 installations comprise the local distribution network (COMSEC accounts) and Tier 3 is where keying material is transferred from the EKMS infrastructure to the consumers End Cryptographic Units (ECUs).

EKMS improved protection of national security-related information by substantially enhancing confidentiality, integrity, and non-repudiation characteristics over the legacy manual key management systems. EKMS has and continues to greatly accelerate availability of crypto key materials through electronic transmission through Public Switched Telephone Network (PSTN) versus the manual handling and shipping of materials. While the current EKMS level-of-effort is directed at enhancing current and developing systems, the ultimate goal is for it to seamlessly transition to the net-centric DoD Key Management Infrastructure (KMI), currently scheduled to begin in FY2012. The AFEKMS Program continues to provide software development to support emerging requirements during the KMI transition period. Activities also include studies and analysis to support both current program planning and execution and future program planning.

This program is in Budget Activity 7, Operational System Development, these budget activities include development efforts to upgrade systems currently fielded or has approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

NOTE: Software development (e.g., Data Management Device - DMD, Common User Application Software - CUAS, and Simple Key Loader - SKL) is rolled up into Tier 2/Tier 3 Development. Software upgrades can be bundled and tracked as a unit, thereby allowing less management overhead and more focus on configuration management and control.

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Title: Tier 2/Tier 3 Software Modification	3.725	1.406	1.651	-	1.651

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force				DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>		PROJECT 674861: <i>EKMS (Electronic Key Management System)</i>		
B. Accomplishments/Planned Programs (\$ in Millions)						
Description: Software modification that address emerging requirements for Tier 2 (base COMSEC account)/Tier 3 (Key material field devices)						
FY 2011 Accomplishments: Software incorporated into the next software release for Tier 2/Tier 3 cryptographic devices (e.g., CUAS and DMD). Ensured the emerging requirements identified in FY 10 as well as those requirements due in FY 11 met operational timelines.						
FY 2012 Plans: Continue to update software releases for Tier 2/Tier 3 EKMS cryptographic devices in order to deliver software enhancements for AF Systems emerging requirements identified in FY 11 and requirements due in FY 12. These components require software upgrades until such time as KMI is capable of providing support to the respective operational communities.						
FY 2013 Base Plans: Will continue to update software releases for Tier 2/Tier 3 cryptographic devices as development for EKMS continues to ensure emerging requirements identified in FY 12 as well as those requirements due in FY 13 meet operational timelines						
Title: Fill/Load Device						
Description: Fill/Load Device Post Production Software Development						
FY 2011 Accomplishments: Developed, test and evaluated new Simple Key Loader (SKL) User Application Software. Developed SKL load profiles to enable new End Crypto Units the abilities to be loaded using the SKL.						
FY 2012 Plans: Continue to develop, test and evaluate new Simple Key Loader User Application Software and develop SKL load profiles to enable new End Crypto Units the abilities to be loaded using the SKL.						
FY 2013 Base Plans: Will continue to develop, test and evaluate new Simple Key Loader User Application Software and develop SKL load profiles to enable new End Crypto Units the abilities to be loaded using the SKL.						
Accomplishments/Planned Programs Subtotals						
		0.361	0.371	0.382	-	0.382
		4.086	1.777	2.033	-	2.033

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 674861: <i>EKMS (Electronic Key Management System)</i>
--	--	--

C. Other Program Funding Summary (\$ in Millions)

<u>Line Item</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u> <u>Base</u>	<u>FY 2013</u> <u>OCO</u>	<u>FY 2013</u> <u>Total</u>	<u>FY 2014</u>	<u>FY 2015</u>	<u>FY 2016</u>	<u>FY 2017</u>	<u>Cost To</u> <u>Complete</u>	<u>Total Cost</u>
• OPAF, PE 0303140F, Information S...: <i>AFEKMS</i>	8.909	11.223	4.288	0.000	4.288	4.753	2.284	1.154	1.589	Continuing	Continuing

D. Acquisition Strategy

All major contracts within this Project are open to full and open competition with technology knowledge, expertise, and prior experience on similar projects weighted heavily in the evaluation process.

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 674861: <i>EKMS (Electronic Key Management System)</i>

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 674861: <i>EKMS (Electronic Key Management System)</i>

Schedule Details

Events	Start		End	
	Quarter	Year	Quarter	Year
AFEKMS Tier 2/3 SW Modification and Updates	1	2011	4	2014
Fill/Load Device Post Production SW Development	4	2011	4	2017

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force									DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>				R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>				PROJECT 675100: <i>Cryptographic Modernization</i>			
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
675100: <i>Cryptographic Modernization</i>	103.145	67.387	51.086	-	51.086	67.233	56.841	63.888	68.032	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Cryptographic Modernization Program modernizes cryptographic devices protecting critical information across the cyber domain operations and national security. In September 2000, the Defense Review Board (DRB) tasked National Security Agency (NSA) to evaluate the security posture of the cryptographic inventory. Systems with aging algorithms, those approaching non-sustainability, and those generally incompatible with modern key management systems were identified. Priority systems that required immediate replacement were also identified. In addition, NSA documented the need to modernize the cryptographic inventory with capabilities designed to enable network-centric operations. Replacements/Modernization of the near term vulnerable systems must occur within the timeframe specified in Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. The DoD Cryptographic Modernization Program was established to develop a modern cryptographic base that provides assured security robustness, interoperability, advanced algorithms, releasability, programmability, and compatibility with the future Key Management Infrastructure (KMI). The program supports an integrated effort across the cyber domain to transform to next generation cryptographic capabilities providing U.S. forces and multinational and interagency partners the security needed to protect the flow and exchange of operational decision making information in accordance with national and international policy/standards, the validated operational requirements of the warfighters, and the Intelligence Communities.

The Cryptographic Modernization Program is a collection of projects accomplished in three phases: replacement, modernization, and transformation. The replacement phase of the program focused on updating and/or replacing out-of-date algorithms along with unsustainable cryptographic products. The modernization phase provides crypto devices with common solutions that are more robust, modular, scalable, and provide the durability to existing cryptographic end items, as well as updating mid-term aging/unsupportable crypto equipment. Manpower and logistics requirements will be reduced and manpower efficiencies gained, while incremental capability enhancements and footprint reduction are provided. The third phase of the Cryptographic Modernization Program, transformation, provides common joint solutions which enable secure transparent network-centric capabilities across the cyber domain. Activities also include studies and analysis to support both current program planning and execution and future program planning.

This program is in Budget Activity 7, Operational System Development, these budget activities include development efforts to upgrade systems currently fielded or has approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Title: KG-3X	0.224	-	-	-	-

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force				DATE: February 2012	
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>		PROJECT 675100: <i>Cryptographic Modernization</i>	
B. Accomplishments/Planned Programs (\$ in Millions)					
Description: KG-3X Develops and acquires Cryptographic Modernization (CM) to replace the aging cryptographic capability for the KG-30 CLOCK START system, part of the Nuclear Command and Control, Minimum Essential Emergency Communications Network.					
FY 2011 Accomplishments: Completed KG-3X CM development and test efforts of replacement crypto devices.					
Title: Remote Rekey (RRK)					
Description: The Remote ReKey program will develop, acquire and install replacement of the CI-13 cryptographic system at remote and unmanned North American Aerospace Defense Command (NORAD) surveillance sites. Sites facilitate NORAD's aerospace control ensuring air sovereignty and air defense of the airspace of the United States. Modernized RRK system complements Identification Friend or Foe (IFF) Mode 5 system upgrade and will distribute cryptographic key for 14 different end cryptographic units. The RRK system is net ready and compatible across multiple communication paths.					
FY 2011 Accomplishments: Continued development and initiate test efforts of replacement cryptographic system.					
FY 2012 Plans: Complete development and test efforts of replacement cryptographic system. Continue working towards certification expected May 2012.					
Title: VINSON/ANDVT Cryptographic Modernization (VACM)					
Description: VINSON/ANDVT Cryptographic Modernization will develop and acquire cryptographic capability to replace the legacy capability on VINSON/ANDVT secure voice communications on aircraft, ships, and ground fixed and mobile platforms (Devices: KY-57/58, KY-99/100, KYV-5 and ARC-234 with Embedded Crypto).					
FY 2011 Accomplishments: Continued software and hardware development leading to System Requirements Review (SRR), Preliminary Design Reviews. Continued ARC 234 modification development using VACM technology.					
FY 2012 Plans:					
	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
	31.162	3.853	-	-	-
	23.027	31.278	30.752	-	30.752

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force			DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675100: <i>Cryptographic Modernization</i>			
B. Accomplishments/Planned Programs (\$ in Millions)					
and transition to development. Initiate Trusted Computing studies and development. Initiate DGK certification efforts. Fund core engineering and database support to the Crypto Modernization portfolio. Initiate and conclude technical solution analysis for High Assurance COTS Mobility (HACM).					
FY 2013 Base Plans: Will continue efforts for MLS Deployment Enablers and MLS Formal Methods Toolsets. Will transition MLS Multi-Core Processor research to development. Will conclude MLS RTOS Graphic Controller development and DGK certification. Continue Trusted Computing development. Will fund core engineering and database support to the Crypto Modernization portfolio. Will initiate MLS Trusted Labeling Interoperability Standard development. Initiate development of HACM.					
Title: TECHNICAL DEVELOPMENT					
Description: Technology Development plans and executes technology maturation and initiates developmental programs to meet emerging and existing warfighter requirements. Includes: Mini Crypto Secure Micro-digital Data Link (SMDDL), Type 1 Data at Rest (T1DAR), Remote Operational Management of End-crypto-units (ROME), Multi-Level Security (MLS) Multi-Port Crypto (MPC) Development, Advanced Message Oriented Data Security Module (AMODSM), and Minuteman Entry Encryption Device (MEED).					
FY 2011 Accomplishments: Completed development and testing of the Mini crypto SMDDL module. Completed ROME Internet Engineering Task Force standard effort and continued development of Reference Implementation. Initiated technology development activities supporting T1DAR. Demonstrated two vendor MLS MPC prototypes.					
FY 2012 Plans: Initiate and complete NSA certification of the SMDDL module and MLS MPC. Initiate development/competitive prototyping effort for a T1DAR solution and Advanced Message-Oriented Data Security Module (AMODSM). Complete Missile Electronic Encryption Device (MEED) study efforts. Continue development of ROME Reference Implementation. Mini Crypto continues under separate effort beginning in FY13.					
FY 2013 Base Plans: Will continue/complete development/competitive prototyping effort for a T1DAR and AMODSM solutions. Will initiate MEED development. Will initiate implementation of the T1DAR solution for specific uses (flight data recorders, EW pods, AWACS). Will complete MLS MPC development and initiate testing. Will complete ROME					
	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
	14.873	7.086	1.143	-	1.143

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675100: <i>Cryptographic Modernization</i>
--	--	--

B. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Reference Implementation development. Breakout development of Mini Crypto High Assurance DDL into separate program line.					
Title: MINI CRYPTO Description: Mini Crypto plans to develop common miniaturized cryptographic solution(s) for use in protecting Secret and Below information on Size, Weight, and Power (SWaP) constrained platforms. FY 2013 Base Plans: Break out from Tech Development. Will continue development of common miniaturized cryptographic solution(s) for use in protecting Classified information on Size, Weight, and Power (SWaP) constrained platforms.	-	-	3.067	-	3.067
Title: SPACE MODULAR COMMON CRYPTO (SMCC) Description: Space Modular Common Crypto develops a modular approach to building NSA Type I cryptographic Aerospace Vehicle Equipment products with configurable functionality to quickly address various COMSEC and TRANSEC requirements. End products allow mixing and matching of modules to meet specific user requirements. FY 2013 Base Plans: Will continue development of Space Modular Common Crypto solutions for Cubesat and large satellite applications including future TT&C, Space Mission Data, TRANSEC and secure network connectivity (e.g. HAIPE, IPSEC). Hold Material Development Decisions, initiate Technology Development activities.	-	-	6.388	-	6.388
Accomplishments/Planned Programs Subtotals	103.145	67.387	51.086	-	51.086

C. Other Program Funding Summary (\$ in Millions)			FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
• OPAF, PE 0303140F, Information S...: <i>Information System Security Program</i>	FY 2011	FY 2012	108.840	0.000	108.840	118.903	24.741	16.572	15.358	Continuing	Continuing

D. Acquisition Strategy
The Crypto Modernization portfolio of component acquisition projects is executing using a variety of approaches that vary from an evolutionary acquisition strategy using spiral development (for new component development) to incremental improvement leveraging leading-edge, certified non-developmental items (for

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force	DATE: February 2012
---	----------------------------

APPROPRIATION/BUDGET ACTIVITY	R-1 ITEM NOMENCLATURE	PROJECT
3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	PE 0303140F: <i>Information Systems Security Program</i>	675100: <i>Cryptographic Modernization</i>

modernization). Contract type is selected for each of the individual projects based upon its acquisition approach and its unique technology risks. A mixture of fixed-price and cost-reimbursement contracts have been selected which maximize the best value for the Government as listed in the R-3.

Program Support Administration (PMA) costs are defined as those direct, unique program costs, other than payroll costs for government personnel, which are required for operation of a program office and its management and oversight role. These include costs such as Advisory and Assistance Service (A&AS) (Specialized Cost Services - SCS, Professional Acquisition Support Services - PASS, Engineering and Technology Acquisition Support Services - ETASS, Federally Funded Research and Development Centers - FFRDC) contracted support to a program office. Under PMA, A&AS personnel support the functions of government personnel in managing a weapon system or common item.

E. Performance Metrics

Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675100: <i>Cryptographic Modernization</i>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675100: <i>Cryptographic Modernization</i>

--	--	--

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675100: <i>Cryptographic Modernization</i>

Schedule Details

Events	Start		End	
	Quarter	Year	Quarter	Year
KG-3X CM development, and test efforts (pg1of2)	1	2011	4	2011
Remote Rekey concept refinement and development (pg1of2)	1	2011	4	2012
VINSON-ANDVT Cryptographic Modernization (VACM) concept refinement and development (pg1of2)	1	2011	4	2013
KG-88 Space Mission Data concept activities and development (pg1of2)	1	2011	2	2012
Space Telemetry Tracking and Commanding (Aerospace Vehicle Equipment [AVE] Increment 1, Carousel, and Ground Operating Equipment [GOE] Increment 1 development (pg1of2)	1	2011	3	2015
F-22 Multifunction Crypto (CM development of KOV-50) and platform integration (pg2of2)	1	2011	4	2011
Concept Refinement (includes MLS, core engineering support, MITRE (pg2of2)	1	2011	4	2017
Technology Development (includes Mini-Crypto, T1DAR, MLS MPC, AMODSM, and MEED)(pg2of2)	1	2011	4	2017
Mini Crypto (pg2of2)	1	2013	1	2016
Space Modular Common Crypto (SMCC) (pg2of2)	1	2013	4	2016

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force									DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>				R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>				PROJECT 675231: <i>AF Key Management Infrastructure (AF KMI)</i>			
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
675231: <i>AF Key Management Infrastructure (AF KMI)</i>	6.352	16.471	10.342	-	10.342	10.551	9.536	10.409	10.852	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Air Force Key Management Infrastructure (AF KMI) Program consists of multiple developments supporting the AF requirements/portion of the DoD Key Management Infrastructure (KMI). (The National Security Agency [NSA] acts as the Executive Agency for the DoD KMI Program.) AF KMI, in concert with this overarching DoD KMI Program, will provide a secure and flexible capability for the electronic generation, distribution, accounting, and management of key material and other communications security (COMSEC) materials for all DoD Command, Control, Communications, Computers, and Intelligence (C4I) and for the Services' weapon systems. KMI represents a broad-scale replacement of the current Electronic Key Management System (EKMS). The new KMI will provide capabilities that will allow networked operation in consonance with the Global Information Grid (GIG) and other DoD, fellow Service, and AF enterprise objectives. It thereby will assure a viable support infrastructure for future weapons and C4I programs to incorporate key management into their system designs.

The DoD KMI will greatly improve protection of national, security-related information by substantially enhancing confidentiality, integrity, and non-repudiation characteristics over the legacy Electronic Key Management System. KMI will greatly accelerate the availability of crypto key materials through electronic transmission versus shipping of materials, will enhance mission responsiveness and flexibility, and will eventually take the man "out-of-the-loop" in the distribution of crypto key materials.

The AF KMI Program in concert with the DoD KMI Program is transitioning the Air Force from the legacy EKMS to modern DoD KMI and building the AF KMI Last Mile architecture. This R&D effort includes system engineering and testing to successfully accomplish the transition and defining of the AF KMI Last Mile architecture. AF KMI Transition is supporting the DoD KMI program as it progresses through the development, testing, and production and fielding phase of the DoD KMI Program. AF KMI efforts includes the transitioning of existing key management capabilities to KMI. The AF KMI Last Mile program is a holistic solution integrating the legacy and new and evolving cryptographic programs, materials, products, sources and consumers. The AF KMI Last Mile capabilities include distribution, management, and load of cryptographic materials from the KMI (COMSEC account) to the End Crypto Units (ECUs). It builds the linkage interfaces that will allow KMI systems to communicate and integrates other related developments to meet operational needs. AF KMI Last Mile is currently performing early system engineering and risk reduction activities supporting those capabilities including analysis of existing equipment and developing technologies, concept refinement studies, and prototyping of existing technologies. Activities also include studies and analysis to support both current program planning and execution and future program planning.

In parallel with AFKMI, DoD and the Services are developing a new generation of End Crypto Units (ECUs) under the Joint Crypto Modernization Initiative that will be capable of direct interaction with the KMI. (PE0303140F, BPAC 675100, Cryptographic Modernization, supports this initiative). In some cases these new ECUs, although needing to be supported by KMI, will not be KMI network-connected. "Last mile" transport of black (aka benign, or encrypted) and red (unencrypted) keying material from a KMI client to a new generation ECU or current legacy ECU will need to be handled in the early years by one of two data transfer devices.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675231: <i>AF Key Management Infrastructure (AF KMI)</i>
--	--	--

This program is in Budget Activity 7, Operational System Development, these budget activities include development efforts to upgrade systems currently fielded or has approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
<p>Title: Key Management Infrastructure Transition</p> <p>Description: Support includes architectural planning, systems engineering, and studies and analyses for migration to the Key Management Infrastructure (KMI) (includes acquisition planning, systems integration, engineering support and System Program Office (SPO) support). Transitioning existing key management capabilities to KMI.</p> <p>FY 2011 Accomplishments: Continued architectural planning, systems engineering, and studies and analyses for migration to Key Management Infrastructure development of the Air Force critical path to transition from EKMS to KMI CI-2 by the FOC date. Continued development of the Joint KMI Concept of Operation and the DoD KMI Master Transition Prerequisites documents. Readied deployment of DoD KMI Management Client (MGC) to pilot AF COMSEC accounts.</p> <p>FY 2012 Plans: Continues architectural planning and systems engineering for migration to DoD Key Management Infrastructure CI-2 Spiral 1. Conducts operational testing of KMI CI-2 components such as the Management Client (MGC) in addition to supporting NSA's operational testing plans. Initiates deployment of the DoD KMI MGC to remaining AF COMSEC accounts.</p> <p>FY 2013 Base Plans: Will continue architectural planning, systems engineering, in support of Key Management Infrastructure (KMI) CI-2 Spiral 2 Spin 1. Will continue support testing of DoD KMI CI-2 components as new hardware/software versions are completed. Initiates the transition of existing key management capabilities to KMI.</p> <p>FY 2013 OCO Plans: N/A</p>	4.369	5.768	6.681	-	6.681
<p>Title: Air Force KMI "Last Mile" Increment I</p> <p>Description: Air Force KMI Last Mile early system engineering and risk reduction to include: concept development; for distribution, load and management elements of last mile; studies and analyses for technology possibilities and prototyping efforts for the last mile.</p>	1.983	10.703	3.661	-	3.661

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675231: <i>AF Key Management Infrastructure (AF KMI)</i>
--	--	--

B. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
<p><i>FY 2011 Accomplishments:</i> Monitored and assisted with the coordination of the Concept Development Document. Continued acquisition planning, systems engineering, and studies and analyses for Key Management Infrastructure Last Mile. Developed MS B Plan, scheduled and tracked development of acquisition documents.</p> <p><i>FY 2012 Plans:</i> Continue early system engineering activities and acquisition planning for the KMI LM. Focus on acquisition planning, system engineering, and concept development to support KMI LM system acquisition. Conduct pre-MS B activities to develop and support an acquisition plan spotlighting cost, performance, and schedule.</p> <p><i>FY 2013 Base Plans:</i> Will continue acquisition planning and system engineering to mature the proposed system concepts to meet the CDD requirements and complete MS B documentation in preparation for system development.</p> <p><i>FY 2013 OCO Plans:</i> N/A</p>					
Accomplishments/Planned Programs Subtotals	6.352	16.471	10.342	-	10.342

C. Other Program Funding Summary (\$ in Millions)											
<u>Line Item</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013 Base</u>	<u>FY 2013 OCO</u>	<u>FY 2013 Total</u>	<u>FY 2014</u>	<u>FY 2015</u>	<u>FY 2016</u>	<u>FY 2017</u>	<u>Cost To Complete</u>	<u>Total Cost</u>
• OPAF, PE 0303140F, Information S...: <i>AF KMI</i>	1.680	7.400	8.591	0.000	8.591	11.631	14.761	11.229	12.331	Continuing	Continuing

D. Acquisition Strategy
All major contracts within this project are open to full and open competition with technology knowledge, expertise, and prior experience on similar projects weighted heavily in the evaluation process.

E. Performance Metrics
Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675231: <i>AF Key Management Infrastructure (AF KMI)</i>

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 675231: <i>AF Key Management Infrastructure (AF KMI)</i>

Schedule Details

Events	Start		End	
	Quarter	Year	Quarter	Year
Architectural Planning, System Engineering and Key Management Transition Support	1	2011	4	2017
AF KMI Last Mile Increment 1	1	2011	2	2016
AF KMI Last Mile Increments 2&3	4	2015	4	2017

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force								DATE: February 2012			
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>				R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>				PROJECT 677820: <i>Computer Security RDT&E: Firestarter</i>			
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
677820: <i>Computer Security RDT&E: Firestarter</i>	9.765	6.022	5.672	-	5.672	5.853	5.961	6.181	6.290	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Firestarter program provides technical transition opportunities for research in the area of Information Assurance (IA) technologies and tools needed to defend Air Force Command, Control, Communications, Computer, and Intelligence (C4I) systems from Information Warfare (IW) attacks, and ensure recovery in the event of an attack. The emphasis of the program is directed toward defensive cyber operations; computer and network systems security; damage assessment and recovery; cyber threat recognition, attribution, and mitigation; and active response methodologies in response to evolving threats and changes to cyber environment. These areas of emphasis are realized through research and development in the areas of: cyberspace surveillance; cyber indications and warning (CI&W); high-speed and host-based network intrusion detection; fusion and correlation of cyber intelligence; decision support; recovery; digital forensics; active response, etc. Current Air Force systems, such as the Combat Information Transport System/Base Information Protection (CITS/BIP) leverage this technology to meet their information assurance needs/requirements. Additionally, this program utilizes IA and cyber technology investments by the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), Director of National Intelligence (DNI), Intelligence Advanced Research Projects Activity (IARPA), and the Department of Homeland Security (DHS) to jump-start its development of solutions to existing Air Force IA and cyber requirements.

This program coordinates and cooperates with 24th AF (AF component to Cyber Command (CYBERCOM)), Joint Task Force - Global Network Operation (JTF-GNO), Strategic Command (STRATCOM), Defense Information Systems Agency (DISA), National Security Agency (NSA) and other services to ensure Global Information Grid (GIG) IA requirements are being met. Activities performed include those designed to identify, analyze, test, rapidly acquire, and integrate emerging IA and cyber technology into all regions of the GIG - terrestrial, airborne, and space systems. Activities also include studies and analysis to support both current program planning and execution and future program planning.

This program is in Budget Activity 7, Operational System Development, these budget activities include development efforts to upgrade systems currently fielded or has approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Title: Cyber Forensic Tools & Methodologies	1.009	1.946	1.859	-	1.859
Description: Cyber forensic tools & methodologies. Includes: Initial metrics for reliable info assurance; secure coalition IA data management, collaboration and visualization; analysis of cyber security bots.					
FY 2011 Accomplishments:					

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Air Force **DATE:** February 2012

APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 677820: <i>Computer Security RDT&E: Firestarter</i>
--	--	---

B. Accomplishments/Planned Programs (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Will continue development of technologies to detect and attribute distributed computer network attacks, over time and distance, to specific adversaries.					
<p>Title: Transition of IA Technology</p> <p>Description: Transition DARPA/DTO/IARPA/DHS information assurance (IA) technology into AF Information Protection, Detection, & Response architecture. Includes: space systems IA solutions; terrestrial net defense technology development; airborne IP network IA tools; IA/cyber modeling & sim; secure interoperable distributed agent computing.</p> <p>FY 2011 Accomplishments: Extended development and implementation of a terrestrial network defense overarching strategy realized through various US Government IA research programs.</p> <p>FY 2012 Plans: Continue enhancing and transitioning customer funded IA technology to operational USAF components in accordance with rapid requirements documentation provided by Air Force Space Command (AFSPC).</p> <p>FY 2013 Base Plans: Will continue enhancing and transitioning customer funded IA technology to operational USAF components in accordance with rapid requirements documentation provided by AFSPC.</p>	6.075	0.979	0.994	-	0.994
Accomplishments/Planned Programs Subtotals	9.765	6.022	5.672	-	5.672

C. Other Program Funding Summary (\$ in Millions)

<u>Line Item</u>	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	<u>Cost To Complete</u>	<u>Total Cost</u>
• N/A: N/A	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing

D. Acquisition Strategy
All major contracts within this project are awarded after full and open competition utilizing evolutionary capability and incremental development.

E. Performance Metrics
Please refer to the Performance Base Budget Overview Book for information on how Air Force resources are applied and how those resources are contributing to Air Force performance goals and most importantly, how they contribute to our mission.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 677820: <i>Computer Security RDT&E: Firestarter</i>

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Air Force		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY 3600: <i>Research, Development, Test & Evaluation, Air Force</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140F: <i>Information Systems Security Program</i>	PROJECT 677820: <i>Computer Security RDT&E: Firestarter</i>

Schedule Details

Events	Start		End	
	Quarter	Year	Quarter	Year
Cyber forensic tools and methodologies	1	2011	4	2017
Cyber Threat Recognition	1	2011	4	2017
Cyber Threat Attribution and Mitigation	1	2011	4	2017
Transition of IA technologies	1	2011	4	2017