Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Air Force											Date: March 2014	
Appropriation/Budget Activity 3600: *Research, Development, Test & Evaluation, Air Force* / BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*							
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
Total Program Element	-	60.837	74.530	70.497	-	70.497	86.005	65.198	53.590	54.465	Continuing	Continuing
674861: *EKMS (Electronic Key Management System)*	-	1.844	2.059	0.592	-	0.592	0.629	0.928	0.947	0.964	Continuing	Continuing
675100: *Cryptographic Modernization*	-	44.483	62.064	60.543	-	60.543	75.249	53.656	41.821	42.472	Continuing	Continuing
675231: *AF Key Management Infrastructure (AF KMI)*	-	9.365	10.407	9.362	-	9.362	10.127	10.614	10.822	11.029	Continuing	Continuing
677820: *Computer Security RDTE: Firestarter*	-	5.145	-	-	-	-	-	-	-	-	Continuing	Continuing

The FY 2015 OCO Request will be submitted at a later date.

Note

In FY 2014, Project 677820, Computer Security Firestarter efforts were transferred to PE 0208088F, Air Force Defensive Cyberspace Operations to better align efforts.

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) 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, ISSP funds the AF operation of one of two Department of Defense (DoD) Tier 1 key distribution centers, and a special computer security program, designated FIRESTARTER. The AF and the DoD require the capability to secure, collect, process, store, and disseminate an uninterrupted flow of information, while denying an adversary the ability to intercept, collect, destroy, interpret, or manipulate our information flows. Secure communication allows the DoD to achieve and maintain decision superiority; the key to successful application of the military instrument of national power. AF COMSEC equipment protects information such as, warfighter positions, mission planning, target strikes, commanders' orders, intelligence, force strength, and force readiness. This COMSEC program ensures adversaries cannot interpret, manipulate, or destroy information. When an adversary is capable of interpretation, manipulation, or destruction of the information used by the warfighter, DoD military forces will suffer significant and/or devastating mission degradation that can result in loss of life and resources and/or cede information that could be used against the United States in a public forum.

The overall focus of the Research, Development, Test, and Evaluation (RDT&E) efforts within this program is to transform electronic key delivery and cryptographic devices to meet the next generation warfighting requirements. These efforts are driven by the National Security Agency's (NSA) 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/interruption 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).

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Air Force	Date: March 2014
Appropriation/Budget Activity 3600: *Research, Development, Test & Evaluation, Air Force* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*

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

B. Program Change Summary ($ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	69.133	90.231	79.946	-	79.946
Current President's Budget	60.837	74.530	70.497	-	70.497
Total Adjustments	-8.296	-15.701	-9.449	-	-9.449
• Congressional General Reductions	-0.091	-0.394			
• Congressional Directed Reductions	-	-25.307			
• Congressional Rescissions	-	-			
• Congressional Adds	-	10.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-1.784	-			
• Other Adjustments	-6.421	-	-9.449	-	-9.449

Change Summary Explanation

Reductions in FY13 Other Adjustments was due to Sequestration.

Congressional Directed Reductions in FY14: (-$3.9M)Concept Refinement and (-$21.407M) Program Decrease.
There was also a Congressional Add (+$10M) for ASACoE in FY14.

Reductions in FY15 funding due to higher Air Force priorities.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force			Date: March 2014
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*	Project (Number/Name) 674861 / *EKMS (Electronic Key Management System)*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
674861: *EKMS (Electronic Key Management System)*	-	1.844	2.059	0.592	-	0.592	0.629	0.928	0.947	0.964	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Air Force Electronic Key Management System (AFEKMS) 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, with users across DoD Command, Control, Communications, Computers, and Intelligence (C4I) and all current AF weapon systems. Bases and units, in garrison and deployed 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). Additionally, AFEKMS resources provide maintenance/distribution of AF Communications Security (COMSEC) publications for all AF users.

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). 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.

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 2013	FY 2014	FY 2015
Title: Tier 2/Tier 3 Software Modification	1.420	1.627	0.245

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 674861 / *EKMS (Electronic Key Management System)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Description: Software modification that address emerging requirements for Tier 2 (base COMSEC account)/Tier 3 (Key material field devices) ***FY 2013 Accomplishments:*** Continued to update software releases for Tier 2/Tier 3 cryptographic devices as development for Electronic Key Management System (EKMS) continues to ensure emerging requirements meet operational timelines ***FY 2014 Plans:*** Will continue to update software releases for Tier 2/Tier 3 cryptographic devices as required by field operations. ***FY 2015 Plans:*** Will continue to update software releases for Tier 2/Tier 3 cryptographic devices as required by field operations.			
Title: Fill/Load Device ***Description:*** Fill/Load Device Post Production Software Development ***FY 2013 Accomplishments:*** Continued to develop, test and evaluate new Simple Key Loader (SKL) User Application Software and develop SKL load profiles to enable new End Crypto Units the abilities to be loaded using the SKL. ***FY 2014 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 2015 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.	0.424	0.432	0.347
Accomplishments/Planned Programs Subtotals	1.844	2.059	0.592

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• OPAF:BA03: 831010: *COMSEC Equipment*	4.282	4.753	2.222	-	2.222	1.102	1.547	1.574	1.603	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 674861 / *EKMS (Electronic Key Management System)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost

Remarks

Other Program Funding reflects Air Force Electronic Key Management System (AFEKMS) portion of Information Systems Security Program (ISSP) OPAF total.

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.

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 674861 / *EKMS (Electronic Key Management System)*

AF EKMS Schedule

Concept activities Design / development Production / fielding

1

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force			Date: March 2014
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*	Project (Number/Name) 675100 / *Cryptographic Modernization*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
675100: *Cryptographic Modernization*	-	44.483	62.064	60.543	-	60.543	75.249	53.656	41.821	42.472	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The AF Cryptographic Modernization Effort modernizes cryptographic devices protecting critical national security information across cyber domain operations. 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 also identified and have been replaced or are being fielded. 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 by device and algorithm in Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. The DoD Cryptographic Modernization Program was established to develop a modern cryptographic base that provides this assured security robustness, interoperability, advanced algorithms, releasability, programmability, and compatibility with the future Key Management Infrastructure (KMI). This AF effort 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 AF Cryptographic Modernization Effort 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. FY14 funding increased to address pending crypto key/algorithm decertifications due to increased threats identified by NSA.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Remote Rekey (RRK)	0.409	-	-
Description: The Remote ReKey (RRK) program will develop, acquire and install a 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. Modernize RRK			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
system complements Identification Friend or Foe (IFF) Mode 5 system upgrade and distribute cryptographic key for 14 different end cryptographic units. The RRK system is net ready and compatible across multiple communication paths. ***FY 2013 Accomplishments:*** Completed development and test efforts. Received Milestone C permission to enter Production and Deployment phase. ***FY 2014 Plans:*** N/A ***FY 2015 Plans:*** N/A			
Title: VINSON/ANDVT Cryptograhic Modernization (VACM) ***Description:*** VINSON/Advanced Narrowband Digital Voice Terminal (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 2013 Accomplishments:*** Continued development and initiated testing and test production representative engineering models, perform NSA certification testing and developmental testing. Continued ARC-234 modification development using VACM technology. ***FY 2014 Plans:*** Will complete engineering manufacturing development and initiate production of 100 Low Rate Initial Production (LRIP) VACM units (to be delivered in FY14/15). Will complete ARC-234 modification development using VACM technology. ***FY 2015 Plans:*** Will complete Force Development Evaluation to test and evaluate the VACM devices.	26.628	19.367	0.091
Title: Space Telemetry Tracking & Commanding (TT&C) Aerospace Vehicle Equipment Increment 1 (AVE Inc1) ***Description:*** Space TT&C AVE Inc 1 develops and delivers space qualified cryptographic products to satellite platforms for securing the TT&C link. ***FY 2013 Accomplishments:*** Continued efforts to implement new algorithms in response to NSA mandates. CAROUSEL replaces CARDHOLDER algorithm. Will award Space TT&C AVE Inc 1 CAROUSEL cryptographic engine (CCE) development contract modification; FY2014 CCE contract modification will be accomplished using active year	2.115	4.325	8.156

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
(FY13) incremental funding. ***FY 2014 Plans:*** Will continue development activities on Space TT&C AVE Inc 1 CCE contract. ***FY 2015 Plans:*** Will continue development activities on Space TT&C AVE Inc 1 CCE contract.			
Title: Technical Development (TD) ***Description:*** Technical Development (TD) refines and develops critical technologies related to evolving threats and Communications Security (COMSEC) capability gaps across AF mission areas. Develops, plans and executes technology maturation efforts to mitigate risk for thousands of users affected by algorithm security issues and ensure required security upgrades can be integrated into the AF enterprise. Works with NSA and other services to develop standards that increase security of communication and information products and facilitate efficient crypto and COMSEC enterprise management. Includes but is not limited to: Secure Micro-digital Data Link (SMDDL), Classified Data at Rest (CDAR), Remote Operational Management of End-crypto-units (ROME), High Assurance Commercial-off-the-Shelf (COTS) Mobility (HACM), Combat Training System Encryption (CTSE), and Enhanced Firefly (EFF) replacement development. TD will also ensure the AF continues providing Distributed Common Ground System (DCGS) Crypto to support the rigorous speed and quality of service requirements of the AF DCGS global Intelligence, Surveillance, and Reconnaissance (ISR) Wide Area Network (WAN) Weapon System (AN/GSQ-272). AF DCGS is based on legacy Asynchronous Transfer Mode (ATM) technologies that are no longer available from manufacturers. DCGS crypto will develop and procure cryptographic devices that allow AF DCGS to continue operating during and after an AF DCGS Communications Modernization from ATM to the Next Generation Deterministic Protocol (NGDP). ***FY 2013 Accomplishments:*** Accomplished pre-MS B activities and continued development of common miniaturized cryptographic solution(s) for use in protecting Classified information on Size, Weight, and Power (SWaP) constrained platforms. Moved development of Mini Crypto high assurance crypto device into separate program line. Conducted SMDDL development, test, and certification activities. Funded CM analysis tool database support to the CM community. Developed ROME Common Crypto Management Information Base (MIB) identifying the framework for future common management of cryptographic devices. Conducted annual assessment of the state of the AF cryptographic enterprise. Began analysis of feasibility of common modular cryptographic solutions for the air and ground environment. ***FY 2014 Plans:*** Will accomplish CTSE requirements refinement and acquisition strategy in partnership with the P5 SPO at Eglin AFB. Will complete SMDDL certification. Will evaluate HACM technologies and track secure mobility solutions impacting AF users. Will investigate classified Data At Rest solutions for tactical environments. Will begin planning replacement of legacy crypto in Air	9.537	20.062	15.931

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Force Distributed Common Ground System (DCGS-AF). Will plan a Link 16 cryptographic upgrade kit procurement. Will begin planning replacement or upgrade of 150,000 Air Force devices that incorporate EFF keying material. Will initiate development of Common Encryption Management software for disparate families of Internet Protocol (IP) encryptors. Will continue the analysis of common modular cryptographic solutions for the air and ground environment. Will support MLS Multi-Domain Simultaneous Access to Virtual Environments (MD SAVE) Joint Capability Technology Demonstration. Application Software Assurance Center of Excellence (ASACoE) had a Congressional Mark of +$10M for FY14. The Technical Development line will include this Congressional Mark of +$10M for ASACoE. ***FY 2015 Plans:*** Will continue HACM and CDAR development. Will finalize plans for the cryptographic portion of Link 16 upgrades. Will continue planning and begin executing replacement or upgrade of 150,000 Air Force devices that incorporate EFF-based keying material. Will continue development of Common Encryption Management software to manage Internet Protocol (IP) encryptors and develop standards for management of future devices. Will develop the cryptographic devices that allow AF DCGS to continue operating during and after a Communications Modernization from ATM to the Next Generation Deterministic Protocol.			
Title: Mini Crypto (MC) ***Description:*** Mini Crypto (MC) 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 Accomplishments:*** N/A ***FY 2014 Plans:*** Releasing a Request for Proposal (RFP) for the Engineering & Manufacturing Development (EMD) phase contract. Conducting a Full and Open Competitive Source Selection. ***FY 2015 Plans:*** After a formal Source Selection, a vendor will be selected and the EMD contract will be awarded for the development of MC. Shortly following contract award, the program will hold a kick-off meeting with vendor and officially begin the EMD phase.	-	1.073	4.188
Title: Space Modular Common Crypto (SMCC) ***Description:*** Space Modular Common Crypto (SMCC) provides Information Assurance (IA) services for new satellite architectures via a family of common crypto solutions that integrate Tracking, Telemetry, & Commanding (TT&C), Mission Data (MD), and/or Transmission Security (TRANSEC) key stream functions for the Air Force and Intelligence Community space systems.	5.794	13.591	28.107

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
FY 2013 Accomplishments: Continued pre-Milestone B activities of SMCC solutions for satellite applications including future TT&C, MD, TRANSEC and secure network connectivity (e.g. HAIPE (High Assurance Internet Protocol Encryption), IPSEC (Internet Protocol Security)). Completed Materiel Development Decision. ***FY 2014 Plans:*** Will continue pre-Milestone B activities, development and risk mitigation activities for SMCC solutions. Conduct SMCC Milestone B. Award SMCC Phase I development contract. ***FY 2015 Plans:*** Will continue risk mitigation activities. Continue SMCC Phase I development contract. Award SMCC Phase II development contract.			
Title: Algorithm Transition, Compliance and Support ***Description:*** Algorithm Transition, Compliance and Support provides Information Assurance (IA) Support that performs transition and governance efforts to be able to effectively analyze 30 classified algorithms, thousands of associated COMSEC keying material short titles, and hundreds of equipment types, and track and report algorithm/device integration across the AF. Based on analysis, determines and monitors mitigation strategies; develops and plans technology maturation efforts to ensure new algorithms can be integrated into the AF enterprise. Assesses current state of AF crypto across the enterprise. Develops and maintains a classified CM database system that tracks status of AF crypto device types that is assessible by the CM community via SIPRNET. Efforts support NC3, ISR, all AF platforms, and most ground networks. ***FY 2013 Accomplishments:*** N/A ***FY 2014 Plans:*** Crypto Algorithm Transition efforts are growing in complexity and the management of Crypto/COMSEC is growing similarly. Will begin development on a method and/or process to accurately transition, track, and manage crypto assets and COMSEC across the AF. Will support algorithm transition and governance efforts to effectively track, analyze, and report on AF use of 30 classified algorithms in over 270,000 devices across the AF enterprise comprised of over 300 equipment types/families and requiring thousands of associated COMSEC keying material short titles. Will provide Crypto-Mod analysis database to AF community to assist in annual assessments during long term effort to develop enterprise capabilities based assessment (CBA) to identify management capability gaps. Will conduct annual assessment of the state of the AF cryptographic enterprise. Will evaluate	-	3.200	3.250

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
impacts of the emerging NSA Commercial Solutions for Classified (CSfC) cryptographic development model and its impacts on AF acquisition and sustainment. ***FY 2015 Plans:*** Will continue to support algorithm transition and governance efforts to effectively track, analyze, and report on AF use of 30 classified algorithms in over 270,000 devices across the AF enterprise comprised of over 300 equipment types/families and requiring thousands of associated COMSEC keying material short titles. Will continue analysis and development of a method and/or process to accurately transition, track, and manage crypto assets and COMSEC across the AF. Will provide Crypto-Mod analysis database to AF community to assist in annual assessments during long term effort to develop enterprise capabilities based assessment (CBA) to identify management capability gaps.Will conduct annual assessment of the state of the AF cryptographic enterprise.Will evaluate NSA recommendations for quantum computing resistant encryption.			
Title: Missile Electronic Encryption Device (MEED) Modernization ***Description:*** MEED was formerly accomplished under the TechnicalDevelopment Major Thrust as a Crypto Mod activity. To increase program transparency MEED will become an acquisition effort. MEED Modernization will modernize the legacy Missile Entry Control System (MECS) devices used to securely authenticate personnel attempting access to this Nation's ground-based Intercontinental Ballistic Missile (ICBM) facilities. This effort will bring the MEED equipment into compliance with current NSA information assurance (IA) security design guidance. ***FY 2013 Accomplishments:*** N/A ***FY 2014 Plans:*** Will initiate MEED Modernization development and accomplish MDD/project activities ***FY 2015 Plans:*** Will continue MEED Modernization	-	0.446	0.820
Accomplishments/Planned Programs Subtotals	44.483	62.064	60.543

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• OPAF: BA03: 831010: *COMSEC Equipment*	108.697	76.309	38.738	-	38.738	26.354	14.861	19.213	19.558	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost

Remarks

Remarks: Other Program Funding reflects Crypto Modernization (CM) portion of Information Systems Security Program (ISSP) OPAF total.

D. Acquisition Strategy

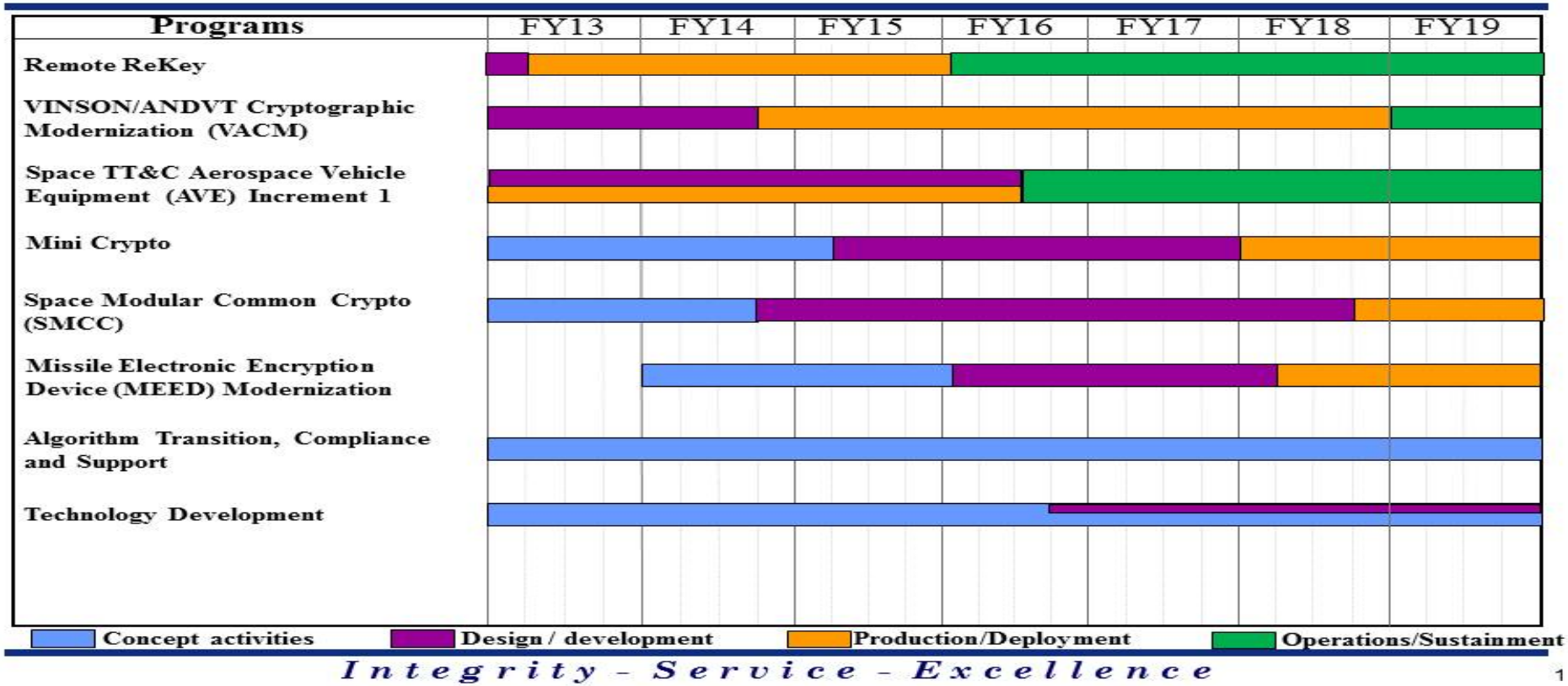
The Crypto Modernization portfolio of component acquisition projects is executing using a variety of approaches that vary from an evolutionary acquisition strategy using spiral development (for new component development) to incremental improvement leveraging leading-edge, certified non-developmental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

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.

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

Cryptographic Modernization Schedule



Integrity - Service - Excellence

1

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force											Date: March 2014	
Appropriation/Budget Activity 3600 / 7					R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*				Project (Number/Name) 675231 / *AF Key Management Infrastructure (AF KMI)*			
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
675231: *AF Key Management Infrastructure (AF KMI)*	-	9.365	10.407	9.362	-	9.362	10.127	10.614	10.822	11.029	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

AFKMI is listed on the AML. 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). 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 EKMS. 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, development and testing to successfully accomplish the transition and defining and developing 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. Re-engineering of repair parts may be required. 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 in the Technology Development Phase. Activities also include studies and analysis to support both current program planning and execution and future program planning.

In parallel with AF KMI, 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 DoD 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

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Infrastructure (AF KMI)*

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. Initial early systems engineering must also be addressed to accommodate future connectivity between the DoD KMI and future KMI Aware/Enabled ECUs. This enabling form factor functionally defined as a common ECU KMI aware/enabled key load module. This is targeted to be a standardized module to be provided to ECU developers and, as such, it must precede any future ECU developments.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
Title: Key Management Infrastructure Transition	5.598	5.588	1.661
Description: Support included architectural planning, systems engineering, testing 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). Transitioned existing key management capabilities to KMI. ***FY 2013 Accomplishments:*** Continued architectural planning, systems engineering, in support of KMI CI-2 Spiral 2 Spin 1. Continued support testing of DoD KMI CI-2 components as new hardware/software versions are completed. Initiated the transition of existing key management capabilities to KMI. ***FY 2014 Plans:*** Will continue architectural planning, systems engineering, in support of 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. ***FY 2015 Plans:*** Will continue architectural planning, systems engineering, testing and studies & analysis in support of KMI CI-2 Spiral 2 Spin 1 and 2. Will continue support testing of DoD KMI CI-2 components as new hardware/software versions are completed. Continues the transition of existing key management capabilities to KMI.			
Title: Air Force KMI Last Mile	3.767	4.819	7.701
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. ***FY 2013 Accomplishments:*** Completed concept refinement activities. Concept Characterization and Technical Descriptions (CCTDs) and Alternative Supporting Analyses were completed. At the request of HQ AFSPC a Material Development Decision (MDD) was approved to enter into the Technology Development phase. A Technology Development contract was awarded to mature two critical			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Infrastructure (AF KMI)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
technologies to Technology Readiness Level (TRL) 6. Assisted with assembly of AF KMI Last Mile draft Capabilities Development Document (CDD) ***FY 2014 Plans:*** Executing the Technology Development contract, developing the requirements for the Engineering and Manufacturing Development (EMD) phase, and finalizing the associated Milestone B (MS B) documentation. ***FY 2015 Plans:*** Will achieve MS B and will award/manage the EMD contract.			
Accomplishments/Planned Programs Subtotals	9.365	10.407	9.362

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• OPAF: BA03: 831010: *COMSEC Equipment*	8.579	11.606	14.457	-	14.457	10.981	12.131	12.345	12.566	Continuing	Continuing

Remarks

Remarks: Other Program Funding reflects AF Key Management Infrastructure (KMI) portion of Information Systems Security Program (ISSP) OPAF total.

D. Acquisition Strategy

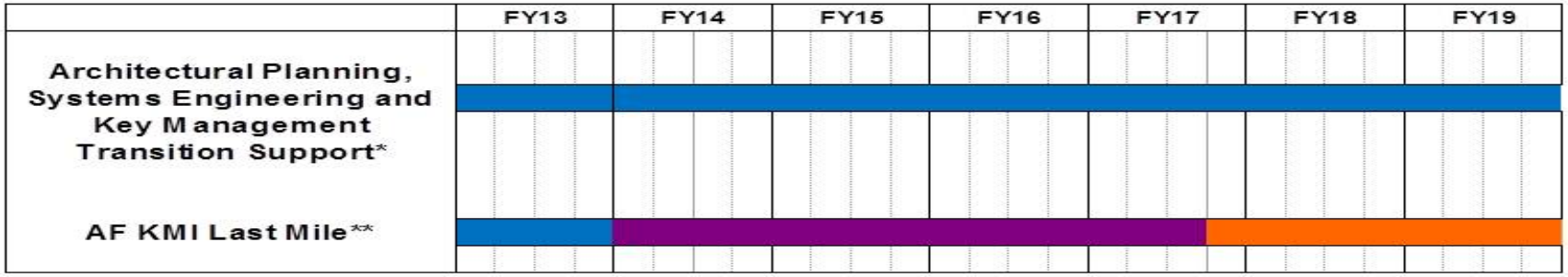
All major contracts within this project are open to full and open competition with technology knowledge, expertise, and prior experience on similar projects weighted heavily in the evaluation process.

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.

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Infrastructure (AF KMI)*

AF KMI Schedule



* Represents the AF planning and migration from EKMS to KMI. AF support is required to accomplish the transition of EKMS Tier 0/1 to KMI: LMD/KP to MGC/AKP and Core Nodes.

** Represents the AF planning, modernization, and procurement of AF KMI systems not replaced by the DoD KMI transition. The new KMI infrastructure creates gaps in existing key management systems supporting over-the-network keying and KMI aware/enabled systems.

Concept activities | Design / development | Production / fielding

1

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force			Date: March 2014
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*	Project (Number/Name) 677820 / *Computer Security RDTE: Firestarter*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
677820: *Computer Security RDTE: Firestarter*	-	5.145	-	-	-	-	-	-	-	-	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

Note

Funding for Project 677820, Computer Security Firestarter efforts, were transferred to PE 0208088F, Air Force Defensive Cyberspace Operations in FY 2014.

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 (AF) 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 2013	FY 2014	FY 2015
Title: Cyber Forensic Tools & Methodologies	1.450	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
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 2013 Accomplishments:*** Continued the development of methods and technologies to enhance "real time" cyber network forensic analysis. ***FY 2014 Plans:*** N/A ***FY 2015 Plans:*** N/A			
Title: Cyber Threat Recognition ***Description:*** Cyber Threat Recognition. Includes: extended effort for info assurance metrics; integrated airborne network security IO platform ***FY 2013 Accomplishments:*** Developed non-signature based detection methods for discovery of malicious network activity. ***FY 2014 Plans:*** N/A ***FY 2015 Plans:*** N/A	1.350	-	-
Title: Cyber Threat Attribution & Mitigation ***Description:*** Cyber Threat Attribution and Mitigation. Includes: risk mitigation techniques for wireless networks and systems; active response, dynamic policy enforcement and computer/net attack attribution efforts. ***FY 2013 Accomplishments:*** Continued development of technologies to detect and attribute distributed computer network attacks, over time and distance, to specific adversaries. ***FY 2014 Plans:*** N/A ***FY 2015 Plans:***	1.440	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2013	FY 2014	FY 2015
N/A			
Title: Transition of IA Technology ***Description:*** Transitions 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. ***FY 2013 Accomplishments:*** Continued to enhance and transition customer funded IA technology to operational USAF components in accordance with rapid requirements documentation provided by AFSPC. ***FY 2014 Plans:*** N/A ***FY 2015 Plans:*** N/A	0.905	-	-
Accomplishments/Planned Programs Subtotals	5.145	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

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.

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Air Force		Date: March 2014
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 677820 / *Computer Security RDTE: Firestarter*

PE 0303140F Project 677820: Firestarter Program Schedule