Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
Total Program Element	-	44.578	46.388	42.973	0.000	42.973	34.871	30.010	11.239	12.469	Continuing	Continuing
674861: *EKMS (Electronic Key Management System)*	-	0.516	0.922	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.438
675100: *Cryptographic Modernization*	-	29.453	38.729	39.712	0.000	39.712	33.407	30.010	11.239	12.469	Continuing	Continuing
675231: *AF Key Management Infrastructure (AF KMI)*	-	14.609	6.737	3.261	0.000	3.261	1.464	0.000	0.000	0.000	0.000	26.071

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 (known as the Key Management Enterprise (KME)). Additionally, ISSP funds the AF operation of its AF KME, one of two Department of Defense (DoD) Tier 1 key distribution centers. ISSP delivers on rising national, DoD, and AF priorities to address cybersecurity threats and increasing warfighter dependence on cyberspace. 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 in modern, high-tempo, full spectrum operations. AF Communications Security (COMSEC) equipment protects information such as warfighter positions, mission planning, target strikes, commanders' orders, intelligence, force strength, and force readiness and 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 exceptionally grave damage to national security.

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) mandates to address decertifications, new requirements, and end of life issues. NSA’s first tenet calls for an AF KME that permits a totally "man-out-of-the-loop" electronic crypto key distribution system from the generation of the key in the key processor all the way into the using End Crypto Unit (ECU). This eliminates the current key vulnerability of compromise/interruption by individuals transporting or loading the key. NSA's second tenet requires an inventory of cryptographic devices that are more robust, modular, scalable, capable, net-centric, and durable. This enables more effective and efficient performance including reduced inventory, expanded data rates, simplified upgrades, lower life cycle costs, and ensured global information grid-compatibility.

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

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force					Date: May 2017
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*			
B. Program Change Summary ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**
Previous President's Budget	46.303	46.388	36.477	0.000	36.477
Current President's Budget	44.578	46.388	42.973	0.000	42.973
Total Adjustments	-1.725	0.000	6.496	0.000	6.496
• Congressional General Reductions	0.000	0.000			
• Congressional Directed Reductions	0.000	0.000			
• Congressional Rescissions	0.000	0.000			
• Congressional Adds	0.000	0.000			
• Congressional Directed Transfers	0.000	0.000			
• Reprogrammings	0.000	0.000			
• SBIR/STTR Transfer	-1.725	0.000			
• Other Adjustments	0.000	0.000	6.496	0.000	6.496

Change Summary Explanation

Increase in FY18 funding to support crypto modernization requirements.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
674861: *EKMS (Electronic Key Management System)*	-	0.516	0.922	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.438
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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 Agent for the DoD EKMS Program. AFEKMS, as part of the AF Key Management Enterprise (KME) and 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 AF weapon systems. AFEKMS supports 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 generation 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 improves 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 via 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 include studies and analysis to support both current program planning and execution as well as development activities to extend life of the Simple Key Loader to bridge the gap between EKMS and the KMI implementation.

NOTE: AF KME 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 2016	FY 2017	FY 2018
Title: Fill /Load Device Post Production SW Development	0.516	0.922	0.000
Description: AF KME Post Production software development focuses on extending life of EKMS through transition to Key Management Infrastructure (KMI) capabilities. This will be accomplished via the Intermediary Application (iApp) software and Tri-Service development of KOV-21 replacement chip through Communications-Electronics Research, Development and Engineering Center (CERDEC) by U.S. Army. The iApp is designed to include all major Data Management Device (DMD)			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
capabilities. The iApp is designed to meet certification and accreditation requirements and iApp user interface is designed for ease of adoption and minimal user training for EKMS DMD, Consolidated Tier 3 Testing Infrastructure (CETTI) User Application Software (UAS), and Simple Key Loader (SKL). The CERDEC effort develops a replacement KOV-21 Card for current Simple Key Loader (SKL) to extend life of SKL until KMI compatible key loader is available. ***FY 2016 Accomplishments:*** - Continued Post Production software for extending life of EKMS through transition to DOD-Level Key Management Infrastructure (KMI) capabilities ***FY 2017 Plans:*** - Continued Post Production software for extending life of EKMS through transition to DOD-Level Key Management Infrastructure (KMI) capabilities. ***FY 2018 Plans:*** - None. No investment activity.			
Accomplishments/Planned Programs Subtotals	0.516	0.922	0.000

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF:BA03: 831010: *COMSEC Equipment*	4.991	10.509	9.127	0.000	9.127	0.000	0.000	0.000	0.000	Continuing	Continuing

Remarks

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

D. Acquisition Strategy

Implement AF portion of the DoD's Cryptographic Modernization(CM) Initiative through modernization/modification efforts, in varying stages of the acquisition cycle, with focus on minimizing life cycle costs. 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-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
675100: *Cryptographic Modernization*	-	29.453	38.729	39.712	0.000	39.712	33.407	30.010	11.239	12.469	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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 in the process of being replaced. 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-See PE 0303140F, BPAC 67523, AF KMI for a full description). This AF effort supports an integrated effort across the cyber domain to transform to next-generation cryptographic capabilities. It provides 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/execution and future program planning.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: VINSON/ANDVT Cryptographic Modernization (VACM)	1.107	0.265	-
Description: VINSON (VHF(Very High Frequency)/UHF(Ultra High Frequency) Wideband Tactical Secure Voice System Cryptographic Equipment)/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptographic Modernization (VACM) 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)).			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
FY 2016 Accomplishments: Completed Force Development Evaluation ***FY 2017 Plans:*** Completed Force Development Evaluation			
Title: Space Telemetry Tracking & Commanding (TT&C) Aerospace Vehicle Equipment Increment 1 (AVE Inc 1) ***Description:*** Space Telemetry Tracking & Commanding (TT&C) Aerospace Vehicle Equipment Increment 1 (AVE Inc 1) develops and delivers space qualified cryptographic products to satellite platforms for securing the TT&C link ***FY 2016 Accomplishments:*** - Completed development activities on Space TT&C AVE Inc 1 Carousel Cryptographic Engine (CCE) contract	0.606	-	-
Title: Technology Development (TD) ***Description:*** Technical Development (TD) conducts concept development and early systems engineering activities to analyze evolving threats and Communications Security (COMSEC) capability gaps across AF and DoD mission areas. Develops, plans and executes foundational technology demonstration efforts to inform COMSEC requirements, build capability roadmaps and support cost estimates prior to Materiel Development Decision (MDD). Mitigates risk for thousands of AF and DoD users affected by algorithm security issues and ensures required security upgrades can be integrated into the AF and DoD enterprise. Works closely 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), Common Encryption Management (CEMENT),Remote Integrated Toolkit (REMIT), Distributed Common Ground System (DCGS) Crypto, Transmission Security (TRANSEC) modernization, Trusted Sensors, Crypto Enterprise Tracking (CET), Advanced Crypto Capabilities (ACC), Trusted Systems Network (TSN)/Supply Chain Risk Management (SCRM), Ground Operating Equipment (GOE) and MILSATCOM Crypto Mod (MCM). ***FY 2016 Accomplishments:*** - Completed development of common crypto management software for integration with Army CHIMERA effort to demonstrate the remote crypto management under CEMENT for disparate families of Internet Protocol (IP) encryptors - Continued analysis for the replacement or upgrade of 150,000 Air Force devices in support of the Advanced Cryptographic Capabilities (ACC) program - Continued analysis of TRANSEC capability gaps and initiate concept characterization study for requirements refinement ***FY 2017 Plans:*** - Continue analysis of TRANSEC capability gaps and CCTDs for requirements refinement	3.086	0.250	0.269

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
- Continue to refine analysis for the replacement or upgrade of 150,000 Air Force devices in support of the Advanced Cryptographic Capabilities (ACC) program - Continue to analyze parts obsolescence, determine crypto modernization requirements, and recommend specific materiel solutions - Assist CCSD Programs with developing their system security documentation (OPSEC Plans, Cybersecurity Plans, Security Classification Guidance (SCG), Integrated Threat Assessments (ITAs), Anti-Tamper Planning and Program Protection Planning. - Continue to evaluate Trusted Sensor candidate solutions for network intrusion detection and prevention. - Develop the necessary TSN processes to deliver a trusted system (integrating all source supply chain information, threat to risk methodologies, mapping of both SCRM Key Practices and RMF mitigations, risk strategies, and technical mitigations for both H/W and S/W). - Provide both counterfeit detection (H/W analysis) and Malware Analysis (S/W analysis). - Assist CCSD programs with TSN contract language and clauses to effectively acquire trusted systems. - Continue to refine analysis for the replacement or upgrade of Ground Operating Equipment (GOE) devices in support of the GOE Initiative and associated activities in support of preparation for Decision Point 2 (DP 2) - Conduct analysis for the replacement or upgrade of legacy MILSATCOM crypto devices in support of the MILSATCOM Crypto Modernization (MCM) Initiative and associated activities in support of preparation for Decision Point 1 (DP1)			
FY 2018 Plans: - Will provide technical guidance in support of ACC operational, testing and evaluation (OT&E) - Will analyze ACC impacts to AF users and provide technical guidance in support of user integration and test - Will refine development/acquisition strategies in support of REMIT phase 3 - Will continue support of AF DCGS network growth and provide technical support to the Program Office - Assist CCSD Programs with developing their system security documentation (OPSEC Plans, Cybersecurity Plans, Security Classification Guidance (SCG), Integrated Threat Assessments (ITAs), Anti-Tamper Planning and Program Protection Planning. - Develop the necessary TSN processes to deliver a trusted system (integrating all source supply chain information, threat to risk methodologies, mapping of both SCRM Key Practices and RMF mitigations, risk			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
strategies, and technical mitigations for both H/W and S/W). - Provide both counterfeit detection (H/W analysis) and Malware Analysis (S/W analysis). - Assist CCSD programs with TSN contract language and clauses to effectively acquire trusted systems. -Will refine development/acquisition strategies in support of GOE Initiative Materiel Development Decision (MDD) - Continue to refine analysis for the replacement or upgrade of legacy MILSATCOM crypto devices in support of the MCM Initiative and associated activities in support of preparation for Decision Point 2 (DP 2), as well as refinement of development/acquisition strategies in support of MCM Initiative MDD.			
Title: Mini Crypto (MC)	5.094	7.777	2.599
Description: Mini Crypto (MC) is developing a Tactical Key Management (TKM) miniaturized cryptographic solution to protect Secret and Below (SaB) Command and Control (C2) and mission data for Size, Weight, and Power (SWaP) constrained platforms which currently have no cryptographic capability and transmit in the clear. MC's TKM solution has a self-generating key which removes the requirement for pre-placed keys and has the ability to add or remove users as tactical situation dictates. ***FY 2016 Accomplishments:*** - Awarded EMD contract. - Completed Integrated Baseline Review (IBR) - Completed System Requirements Review (SRR)/System Functional Review (SFR) - Conducted Preliminary Design Review (PDR) - Delivered prototypes for initial test activities in support of integrated testing ***FY 2017 Plans:*** - Continue to execute the EMD contract -Complete Critical Design Review (CDR) - Accept Production Representative Engineering Development Models (PREDMs) to support Government Integrated -Plan and execute Development/Operational Testing and Operational Assessment - Use PREDMs during this period for Security Verification Testing (SVT) as the program works toward NSA Type 1 Certification. - Update documentation for Milestone C ***FY 2018 Plans:*** - Seek Milestone C approval from PEO - Begin operational testing			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
- Prepare Engineering Change Proposals to address deficiencies identified in testing			
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. ***FY 2016 Accomplishments:*** - Continued Technology Maturation Risk Reduction (TMRR) activities - Achieved MS B in Nov 15 - Awarded SMCC AES-256 Crypto Engine (ACE) Common Solution (ACS) development contract in Apr 16 ***FY 2017 Plans:*** - Continue TMRR and SMCC ACS development contract activities - Awarded SMCC Medium/Largesat Common Solution (MLCS) development contract in Feb 17 ***FY 2018 Plans:*** - Will ramp down TMRR activities - Will complete SMCC ACS development contract activities - Will continue SMCC MLCS development contract activities	11.955	28.052	34.837
Title: Algorithm Transition Compliance and Support ***Description:*** Supports AF Space Command (AF Cyber Core Function Lead) in Algorithm Transition Compliance and Support provides Information Assurance (IA) support that performs transition and governance efforts to effectively analyze 30 classified algorithms, thousands of associated COMSEC keying material short titles, and hundreds of equipment types. This effort also tracks and reports algorithm/device integration across the AF. Analysis determines and monitors mitigation strategies; develops and plans technology demonstration 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 accessible by the CM community via SIPRNET. Efforts support NC3, ISR, all AF platforms, and most ground networks. ***FY 2016 Accomplishments:*** - Supported 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	1.193	0.883	2.007

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
- Continued analysis and development of a method and/or process to accurately transition, track, and manage crypto assets and COMSEC across the AF - Provided 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 - Conducted annual assessment of the state of the AF cryptographic enterprise - Continued to evaluate NSA recommendations for Advanced Cryptographic Capabilities suite of algorithms and identify related tasks which affect the AF ***FY 2017 Plans:*** - 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 - Continue analysis and development of a method and/or process to accurately transition, track, and manage crypto assets and COMSEC across the AF - 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 - Conduct annual assessment of the state of the AF cryptographic enterprise - Continue to evaluate NSA recommendations for Advanced Cryptographic Capabilities suite of algorithms and identify related tasks which affect the AF ***FY 2018 Plans:*** - Will continue to analyze the AF Crypto and Cyber enterprise and provide situational awareness to significant risks related to aging inventory and vulnerabilities to the key exchange process - Will provide assessment of Commercial Solutions for Classified (CSfC) and Quantum Resistance Encryption impacts			

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
- Will continue to provide analysis of adequacy of COMSEC and Cyber products in support of NSA requirements, sustainment issues and the state of technology			
Title: Missile Electronic Encryption Device (MEED) Modification ***Description:*** The MEED Modification upgrades 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 2016 Accomplishments:*** - Awarded MEED Modification EMD contract (First Quarter FY16) ***FY 2017 Plans:*** - Continue to execute the EMD FFP contract - Complete Operational Testing - Release Production RFP for Production contract	4.886	1.402	-
Title: Classified Data At Rest (CDAR) ***Description:*** CDAR plans to develop and procure an NSA approved modernized cryptographic solution(s) for use in ISR, C2, and EW platforms exposed to hostile/uncontrolled environments. The enterprise cryptographic solution will encrypt/decrypt Top Secret and Below (TSAB) data at rest residing in a variety of data storage environments. ***FY 2016 Accomplishments:*** - Continued early systems engineering activities to include market research, platform requirements investigation, studies and analysis, and concept exploration and refinement for potential CDAR solutions ***FY 2017 Plans:*** - Complete early systems engineering and concept development activities leading to Materiel Development Decision (MDD) - Conduct material solution analysis and complete Analysis of Alternatives (AoA)	0.616	0.000	-
Title: Integrated Data Denial (IDD) Crypto ***Description:*** The United States Nuclear Detonation (NUDET) Detection System (USNDS) Program and Air Force Space Command have identified a need to replace the Integrated Data Denial (IDD) crypto devices within the USNDS architecture. The primary purpose of USNDS is to detect, locate, and report nuclear detonation in Earth's atmosphere or near space in near real time. IDD is a cryptographic component within the USNDS ground systems and is currently facing obsolescence issues. ***FY 2016 Accomplishments:***	0.910	0.100	-

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
- Initiative Integrated Product Team (IIPT) formed to refine IDD program objectives, submit funding requirements, conduct studies and analyses, perform risk assessment - Collaborated with SMC/GPGN (USNDS SPO and supported customer) and AFSPC/A5C and CYSS/CYZ to validate IDD modification requirement ***FY 2017 Plans:*** - Continue to analyze parts obsolescence, determine crypto modernization requirements, and recommend specific materiel solution - Conduct IDD Modernization Materiel Development Decision (MDD) - Brief Acquisition Strategy Panel (ASP)			
Accomplishments/Planned Programs Subtotals	29.453	38.729	39.712

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF: BA03: 831010: *COMSEC Equipment*	30.538	21.775	17.780	0.000	17.780	21.957	16.550	24.034	0.000	Continuing	Continuing

Remarks

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

D. Acquisition Strategy

Implement AF portion of the DoD's Cryptographic Modernization(CM) Initiative through modernization/modification efforts, in varying stages of the acquisition cycle, with focus on minimizing life cycle costs. The CM 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-3, RDT&E Project Cost Analysis: FY 2018 Air Force			Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
VINSON/ANDVT Cryptographic Modernization (VACM)	C/CPIF	Raytheon Company : Ft Wayne, IN	-	0.992	Dec 2017	0.240	Dec 2017	0.000		0.000		0.000	0.000	1.232	47.863
VINSON/ANDVT/ Cryptographic Modernization (ARC-234)	MIPR	Defense Microelectronic Activity : Sacramento, CA	-	0.000		0.000		0.000		0.000		0.000	0.000	0.000	32.737
Space Telemetry, Tracking & Commanding (TT&C) Aerospace Vehicle Equipment (AVE Inc 1)	C/CPFF	General Dynamics C4 Systems : Scottsdale, AZ	-	0.235	May 2016	0.000		0.000		0.000		0.000	Continuing	Continuing	-
Tech Development	Various	MULTIPLE : MULTIPLE	-	1.369	Jan 2016	0.250	Jan 2017	0.269	Jan 2018	0.000		0.269	Continuing	Continuing	-
Mini Crypto	C/CPIF	VIASAT, INC : Carlsbad, CA	-	4.380	Oct 2015	6.359	Apr 2017	1.717	Apr 2018	0.000		1.717	0.000	12.456	-
Space Modular Common Crypto (SMCC)	C/CPIF	MULTIPLE : MULTIPLE	-	7.082	Apr 2016	23.766	Feb 2017	27.166	Dec 2017	0.000		27.166	Continuing	Continuing	-
Missile Electronic Encryption Device (MEED) Modernization	C/FFP	SAIC : Tampa, FL	-	3.323	Feb 2016	0.472	Aug 2017	0.000		0.000		0.000	Continuing	Continuing	-
Algorithm Transition, Compliance and Support	C/TBD	MULTIPLE : MULTIPLE	-	0.000		0.183	Apr 2017	0.189	Apr 2017	0.000		0.189	Continuing	Continuing	-
Integrated Data Denial (IDD) Crypto	C/TBD	MULTIPLE : MULTIPLE	-	0.336	Apr 2017	0.100	Apr 2017	0.000		0.000		0.000	Continuing	Continuing	-
		Subtotal	-	17.717		31.370		29.341		0.000		29.341	-	-	-

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		Subtotal	-	-		-		-		-		-	-	-	-

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
VINSON/ANDVT Crypto Mod (VACM)	MIPR	MULTIPLE : MULTIPLE	-	0.115	Dec 2015	0.000		0.000		0.000		0.000	0.000	0.115	5.001
Space Telemetry, Tracking & Commanding (TT&C) Aerospace Vehicle Equipment Increment 1 (AVE Inc 1)	Various	MULTIPLE : MULTIPLE	-	0.330	Nov 2015	0.000		0.000		0.000		0.000	0.000	0.330	-
Mini Crypto	Various	MULTIPLE : MULTIPLE	-	0.339	Mar 2016	0.656	Mar 2017	0.441	Mar 2018	0.000		0.441	Continuing	Continuing	-
Space Modular Common Crypto (SMCC)	Various	MULTIPLE : MULTIPLE	-	1.457	Dec 2015	0.360	Oct 2016	2.153	Dec 2017	0.000		2.153	Continuing	Continuing	-
Missile Electronic Encryption Device (MEED) Modernization	MIPR	MULTIPLE : MULTIPLE	-	0.554	Jul 2016	0.234	Feb 2017	0.000		0.000		0.000	Continuing	Continuing	-
		Subtotal	-	2.795		1.250		2.594		0.000		2.594	-	-	-

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Administration (PMA)	Various	Various : Various	-	8.941	Dec 2015	6.109	Dec 2016	7.777	Dec 2017	0.000		7.777	Continuing	Continuing	-
		Subtotal	-	8.941		6.109		7.777		0.000		7.777	-	-	-

	Prior Years	FY 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	29.453		38.729		39.712		0.000		39.712	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

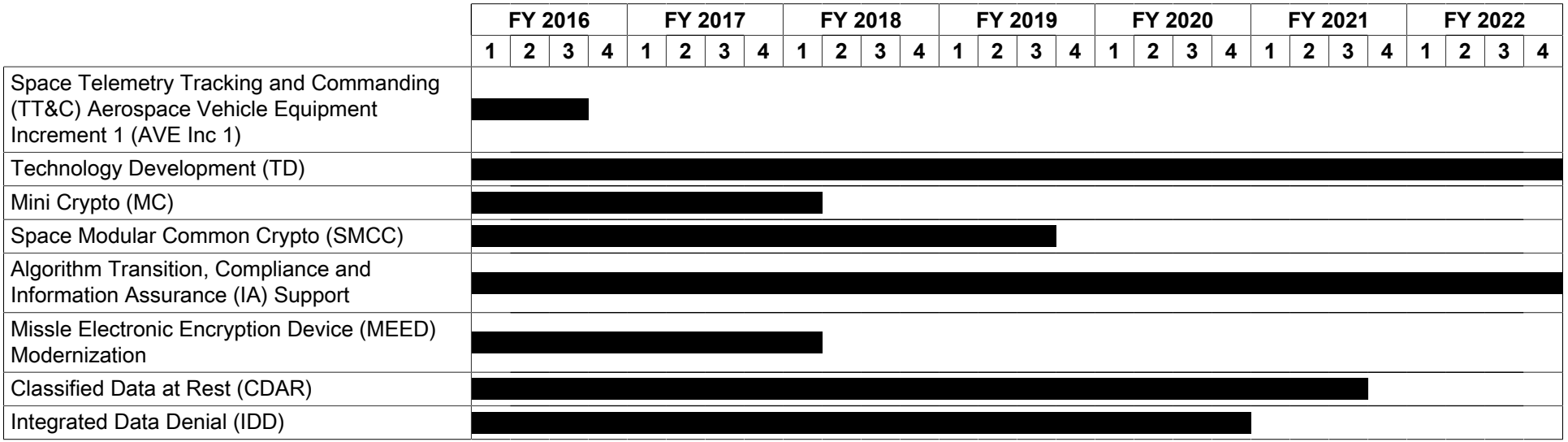

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Air Force		Date: May 2017
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Space Telemetry Tracking and Commanding (TT&C) Aerospace Vehicle Equipment Increment 1 (AVE Inc 1)	1	2016	3	2016
Technology Development (TD)	1	2016	4	2022
Mini Crypto (MC)	1	2016	1	2018
Space Modular Common Crypto (SMCC)	1	2016	3	2019
Algorithm Transition, Compliance and Information Assurance (IA) Support	1	2016	4	2022
Missle Electronic Encryption Device (MEED) Modernization	1	2016	1	2018
Classified Data at Rest (CDAR)	1	2016	3	2021
Integrated Data Denial (IDD)	1	2016	4	2020

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force			Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
675231: *AF Key Management Infrastructure (AF KMI)*	-	14.609	6.737	3.261	0.000	3.261	1.464	0.000	0.000	0.000	0.000	26.071
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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 Agent 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) systems 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 AF Information Network 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 Research and Development effort includes system engineering, development and testing to successfully implement the AF KMI Last Mile architecture as part of the AF Key Management Enterprise (KME). 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 as part of the AF KME distribution, management, and load of cryptographic materials from the KMI (COMSEC account) to the end cryptographic unit (ECU). 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 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 addressing the need for a new generation of future KMI-aware ECU that will be capable of direct interaction with the DoD KMI Enterprise, under the Joint Crypto Modernization Initiative (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. 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.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Air Force		Date: May 2017
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 2016	FY 2017	FY 2018
Title: Air Force KMI Last Mile Space & Naval Warfare Systems Command (SPAWAR) Support(Tier 3) ***Description:*** Support includes 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 AF KMI Last Mile Tier 3. ***FY 2016 Accomplishments:*** - Continued to provide annual resources to SPAWAR to plan and execute specific profiles testing for all Air Force ECUs - Initiated Management Station Application (MS App) development based upon the existing Intermediary Application (iApp) software ***FY 2017 Plans:*** - Continue to provide annual resources to SPAWAR to plan and execute specific profile testing for all Air Force ECUs - Continue MS App development based upon the existing iAPP software ***FY 2018 Plans:*** - Will continue to provide annual resources to SPAWAR to plan and execute specific profile testing for all Air Force ECUs - Will integrate and test MS App with existing Tier 3 key loaders.	1.637	2.116	3.261
Title: Air Force KMI Last Mile (Tier 3) ***Description:*** Air Force KMI Last Mile Tier 3 early system engineering, risk reduction and engineering development 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; and development of a certified KMI-aware, Product Delivery Enclave - enabled key load device. ***FY 2016 Accomplishments:*** - Achieved Critical Design Review for the Portable Key Loader (PKL) EMD contract ***FY 2017 Plans:*** - PKL contract terminated for convenience. ***FY 2018 Plans:*** - Contract terminated in FY17.	12.972	4.621	0.000
Accomplishments/Planned Programs Subtotals	14.609	6.737	3.261

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

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPAF: BA03: 831010: *COMSEC Equipment*	4.452	4.148	8.679	0.000	8.679	9.805	11.242	11.277	12.932	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

Implement AF portion of the DoD's Cryptographic Modernization (CM) Initiative through modernization/modification efforts, in varying stages of the acquisition cycle, with focus on minimizing life cycle costs. 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.