Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Air Force	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	-	35.775	27.726	10.351	0.000	10.351	13.598	13.405	61.566	62.698	Continuing	Continuing
675100: *Cryptographic Modernization*	-	34.322	27.726	10.351	0.000	10.351	13.598	13.405	61.566	62.698	Continuing	Continuing
675231: *AF Key Management Enterprise (AF KME)*	-	1.453	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

Information Systems Security Program (ISSP) - Includes resources, manpower authorizations, necessary facilities and equipment required to perform INFOSEC research and development, to provide INFOSEC services, to procure INFOSEC products required to secure telecommunications and information systems when such products are separately procurable from host systems, and to provide INFOSEC maintenance and support. Also includes costs associated with the protection afforded to telecommunications and information systems which process sensitive data and efforts to ensure confidentiality, integrity, and availability of the information and the system.

The 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)). ISSP delivers on rising national, DoD, and AF priorities to address cyber security threats and increasing war-fighter 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 war-fighter 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 war-fighter, 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 war-fighting 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Air Force	Date: February 2020
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 element may include necessary civilian pay expenses required to manage, execute, and deliver ISSP weapon system capability. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

This program is in Budget Activity 7, Operational System Development because this budget activity includes development efforts to upgrade systems that have been fielded or have received approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

This requirement supports performance of a full financial audit as required by title 10 U.S.C. Chapter 9A, Sec 240-D.

This program is in Budget Activity 7, Operational System Development because this budget activity includes development efforts to upgrade systems that have been fielded or have received approval for full rate production and anticipate production funding in the current or subsequent fiscal year.

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	33.979	27.726	11.156	0.000	11.156
Current President's Budget	35.775	27.726	10.351	0.000	10.351
Total Adjustments	1.796	0.000	-0.805	0.000	-0.805
• 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	3.000	0.000			
• SBIR/STTR Transfer	-1.204	0.000			
• Other Adjustments	0.000	0.000	-0.805	0.000	-0.805

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
675100: *Cryptographic Modernization*	-	34.322	27.726	10.351	0.000	10.351	13.598	13.405	61.566	62.698	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 multi-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 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 Enterprise (KME-See PE 0303140F, Project 67523, AF KME 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 multi-domain security needed to protect the flow and exchange of strategic, operational, and tactical information in accordance with national and international policy/standards, and the validated requirements of decision makers, warfighters, and the intelligence community.

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, multi-domain, network-centric capabilities. Activities also include studies and analysis to support both current program planning/ execution and future program planning.

This program element may include necessary civilian pay expenses required to manage, execute, and deliver ISSP weapon system capability. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Technology Development (TD)	8.372	7.275	3.469
Description: Technical Development (TD) conducts concept development, early systems engineering, and development/ modernization activities to analyze and mitigate evolving crypto threats and Communications Security (COMSEC) capability			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
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 2019	FY 2020	FY 2021
gaps across AF and DoD mission areas. Develops, plans and executes Technology Maturation and Risk Reduction (TMRR) and Engineering and Manufacturing Development (EMD) activities for future cryptographic initiatives. 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. Initiatives include but are not limited to: Advanced Cryptographic Capabilities Increment One (ACC Inc. 1) and Cryptographic Modernization 2 (CM2). ***FY 2020 Plans:*** -Coordinate the AF Limited User Testing (LUT) for the Advanced Cryptographic Capabilities Increment One (ACC Inc.1) initiative -Continue TMRR activities to support cryptographic equipment modifications and new cryptographic equipment developments within the scope of the CM2 initiative -Identify materiel solutions requiring modification or acquisition under the joint CM2 Initial Capabilities Document (ICD) and provide information to AF Lead Command to support AF1067 modifications or JCIDS documentation for follow-on acquisition -Continue development of the Common Cryptologic Management Information Base (CC MIB) standard that will enable accurate tracking and management of crypto assets in support of COMSEC Enterprise Management (EM) and to verify CM2 algorithm transition compliance -Begin the modification of CM2 impacted cryptographic devices to mitigate CM2 associated threats -Continue to develop system security documentation (Operational Security (OPSEC) Plans, Cybersecurity Plans, Security Classification Guidance (SCG), Integrated Threat Assessments (ITAs), Anti-Tamper Planning and Program Protection Planning) -Continue to develop the necessary Trusted System Network (TSN) processes to deliver a trusted system (integrating all source supply chain information, threat to risk methodologies, mapping of both SCRM Key Practices and Risk Management Framework (RMF) mitigations, risk strategies, and technical mitigations for both H/W and S/W) -Continue to provide both counterfeit detection (H/W analysis) and Malware Analysis (S/W analysis) -Continue to provide TSN contract language and clauses to effectively acquire trusted systems ***FY 2021 Plans:*** -Will continue to coordinate AF Limited User Testing (LUT) for the Advanced Cryptographic Capabilities Increment One (ACC Inc.1) initiative -Will continue to identify materiel solutions requiring modification or acquisition under the joint Cryptographic Modernization 2 (CM2) Initial Capabilities Document (ICD) and provide information to AF Lead Command to support AF1067 modifications or JCIDS documentation for follow-on acquisition -Will conduct Technology Maturation and Risk Reduction (TMRR) activities, execute AF 1067 cryptographic equipment modifications, and begin new cryptographic equipment developments within the scope of the CM2 program -Will continue the modification of CM2 impacted cryptographic devices to mitigate CM2 associated threats			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
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 2019	FY 2020	FY 2021
-Will continue development of the Common Cryptologic Management Information Base (CC MIB) standard that will enable accurate tracking and management of crypto assets across the AF in support of the CM2 developments -Will develop system security documentation (OPSEC Plans, Cybersecurity Plans, Security Classification Guidance (SCG), Integrated Threat Assessments (ITAs), Anti-Tamper Planning and Program Protection Planning) -Will 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 Risk Management Framework (RMF) mitigations, risk strategies, and technical mitigations for both H/W and S/W) -Will provide both counterfeit detection (H/W analysis) and Malware Analysis (S/W analysis) -Will provide TSN contract language and clauses to effectively acquire trusted systems ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Funding decreased due to higher AF priorities			
Title: IFF Mode 5	-	4.779	3.274
Description: Identification Friend or Foe (IFF) Mode 5 devices provide authentication and encryption/decryption services to IFF Mode 5 host equipment. These encryption devices operate within military aircraft, fixed, and transportable ground stations when connected to an interrogator and/or transponder. The Identification Friend or Foe (IFF) Mode 5 crypto models KIV-77 and KIV-78 require permanent modification. The modification of these devices are required to address produce-ability and algorithm re-programmability mandated by the National Security Agency (NSA) and the 2019 Chairman of the Joint Chiefs of Staff Notice (CJCSN) 6510. ***FY 2020 Plans:*** -Executing funding from the Technology Development (TD) thrust for the modification of the KIV-78 IFF Mode 5 device in support of the Cryptographic Modernization 2 (CM2) effort as stated in TD description -Establish the CM2 Modification: IFF Mode 5 Program Management Office (PMO) to oversee the development contract ***FY 2021 Plans:*** -Reallocate funding from the Technology Development thrust to execute the permanent modification of the IFF Mode 5 in support of the Cryptographic Modernization 2 (CM2) effort -Execute the modification development effort for the IFF Mode 5 in support of the CM2 effort ***FY 2020 to FY 2021 Increase/Decrease Statement:*** -Funding decreased to execute a permanent modification of the IFF devices to incorporate cryptographic resilience through algorithm re-programmability mandated by the National Security Agency (NSA) and the 2019 Chairman of the Joint Chiefs of Staff			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
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 2019	FY 2020	FY 2021
Notice (CJCSN) 6510. Funding was decreased from TD in order to continue development of the CM2 modification effort under the IFF thrust.			
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 2020 Plans:*** - Ramp down SMCC development contract activities ***FY 2020 to FY 2021 Increase/Decrease Statement:*** - Will complete SMCC EMD Phase	22.306	12.124	-
Title: Algorithm Transition Compliance and Support ***Description:*** Supports Air Combat Command (AF lead for Cyber Superiority) in Algorithm Transition Compliance and provides Information Assurance (IA) support by conducting analysis on all utilized cryptographic algorithms and hundreds of cryptographic equipment types to support transition efforts. This includes the development and planning of technology demonstrations to ensure new algorithms can be integrated into the multitude of devices across the AF crypto enterprise, determining and monitoring mitigation strategies to address vulnerabilities, and tracking and reporting algorithm/device integration. Assesses current state of AF cryptography across the enterprise and develops the Cryptographic Roadmap. Develops and maintains a classified Crypto Modernization (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 2020 Plans:*** -Continue to analyze the AF crypto enterprise and provide situational awareness of significant risks related to aging inventory and cryptographic vulnerabilities -Continue to provide analysis of adequacy of COMSEC products in support of NSA requirements, sustainment issues, and the state of technology -Provide Crypto Mod analysis database to AF community to assist in annual assessments and long term efforts to develop enterprise capabilities based assessment (CBA) and to identify technical capability gaps -Conduct annual assessment of the state of the AF cryptographic enterprise and update the Cryptographic Roadmap ***FY 2021 Plans:***	3.385	3.448	3.508

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
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 2019	FY 2020	FY 2021
- Will continue to analyze the AF crypto enterprise and provide situational awareness of significant risks related to aging inventory and cryptographic vulnerabilities - Will continue to provide analysis of adequacy of COMSEC products in support of NSA requirements, sustainment issues, and the state of technology - Will provide Crypto-Mod analysis database to AF community to assist in annual assessments and long term efforts to develop enterprise capabilities based assessment (CBA) and to identify technical capability gaps - Will conduct annual assessment of the state of the AF cryptographic enterprise and update the Cryptographic Roadmap ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Funding increased due to Cryptographic Modernization 2 (CM2) requirements			
Title: Missile Electronic Encryption Device (MEED) Modification ***Description:*** The MEED Modification upgraded 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 2020 Plans:*** N/A ***FY 2021 Plans:*** N/A	0.159	0.000	0.000
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 2020 Plans:*** - Conduct Risk Reduction and Technology Maturation (TMRR) prototyping of key enabling technologies - Continue market research and preparation for Milestone B and entry into EMD ***FY 2021 Plans:*** - Will complete TMRR prototyping - Will continue market research and preparation for Milestone B and entry into EMD	0.100	0.100	0.100
Accomplishments/Planned Programs Subtotals	34.322	27.726	10.351

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• OPAF 03 831010: *COMSEC Equipment*	53.171	49.979	48.736	-	48.736	49.573	50.438	51.343	52.284	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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Air Force		Date: February 2020
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 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Tech Development	Various	MULTIPLE : MULTIPLE	-	2.393	Jan 2019	14.152	Jan 2020	6.743	Dec 2021	-		6.743	Continuing	Continuing	-
Space Modular Common Crypto (SMCC)	C/CPIF	MULTIPLE : MULTIPLE	-	23.664	Dec 2018	9.383	Feb 2020	-		-		-	0.000	33.047	-
		Subtotal	-	26.057		23.535		6.743		-		6.743	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Space Modular Common Crypto (SMCC)	Various	MULTIPLE : MULTIPLE	-	1.811	Dec 2018	0.743	Dec 2019	-		-		-	0.000	2.554	-
		Subtotal	-	1.811		0.743		-		-		-	0.000	2.554	N/A

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Administration (PMA)	Various	Various : Various	-	6.454	Dec 2018	3.448	Dec 2019	3.608	Dec 2020	-		3.608	Continuing	Continuing	-
		Subtotal	-	6.454		3.448		3.608		-		3.608	Continuing	Continuing	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	34.322		27.726		10.351		-		10.351	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Air Force		Date: February 2020
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

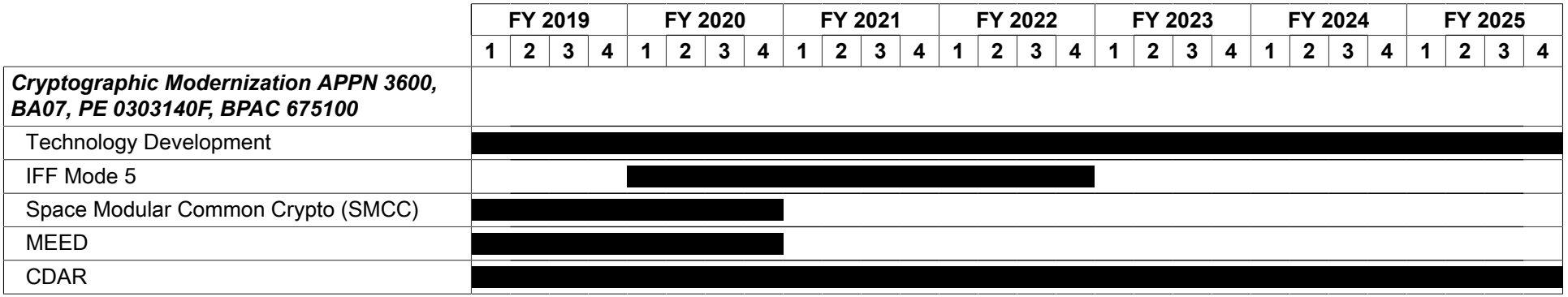

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Air Force		Date: February 2020
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675100 / *Cryptographic Modernization*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Cryptographic Modernization APPN 3600, BA07, PE 0303140F, BPAC 675100				
Technology Development	1	2019	4	2025
IFF Mode 5	1	2020	4	2022
Space Modular Common Crypto (SMCC)	1	2019	4	2020
MEED	1	2019	4	2020
CDAR	1	2019	4	2025

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force			Date: February 2020
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*	Project (Number/Name) 675231 / *AF Key Management Enterprise (AF KME)*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
675231: *AF Key Management Enterprise (AF KME)*	-	1.453	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Air Force Key Management Enterprise (AF KME) Program consists of multiple developments supporting the AF requirements/portion of the DoD Key Management Infrastructure (KMI) at the Tier 3 level. 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 KME Tier 3 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) Tier 3. The AF KME Tier 3 is a holistic solution integrating the legacy and new and evolving cryptographic programs, materials, products, sources and consumers. The AF KME Tier 3 capabilities include as part of the AF KME distribution, management, and loading 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 integrate other related developments to meet operational needs. AF KME Tier 3 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 ECUs 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. Development of these two data transfer devices is supported by the Air Force Key Management Enterprise Tier 3 Program.

This program element may include necessary civilian pay expenses required to manage, execute, and deliver ISSP weapon system capability. The use of such program funds would be in addition to the civilian pay expenses budgeted in program element 0605831F.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Air Force		Date: February 2020
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Enterprise (AF KME)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Air Force KME Tier 3 Network Information Warfare Center (NIWC) Support (Tier 3)	1.453	0.000	0.000
Description: Support includes architectural planning, systems engineering, testing and studies and analyses for Tier 3 Key Management activities (includes acquisition planning, systems integration, engineering support and System Program Office (SPO) support). Transitioned existing key management capabilities to AF KME Tier 3. ***FY 2020 Plans:*** N/A ***FY 2021 Plans:*** N/A			
Accomplishments/Planned Programs Subtotals	1.453	0.000	0.000

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• OPAF 03 831010: *COMSEC Equipment*	2.654	2.623	1.955	-	1.955	2.909	2.960	3.012	3.067	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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2021 Air Force			Date: February 2020
Appropriation/Budget Activity 3600 / 7	R-1 Program Element (Number/Name) PE 0303140F / *Information Systems Security Program*	Project (Number/Name) 675231 / *AF Key Management Enterprise (AF KME)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
AF KMI Last Mile (Tier 3)	C/CPIF	L3 Comm : Camden, NJ	-	1.258	Mar 2019	-		-		-		-	0.000	1.258	13.364
		Subtotal	-	1.258		-		-		-		-	0.000	1.258	N/A

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2019 Cost	FY 2019 Award Date	FY 2020 Cost	FY 2020 Award Date	FY 2021 Base Cost	FY 2021 Base Award Date	FY 2021 OCO Cost	FY 2021 OCO Award Date	FY 2021 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management Administration (PMA)	Various	Various : Various	-	0.195	Dec 2018	-		-		-		-	0.000	0.195	-
		Subtotal	-	0.195		-		-		-		-	0.000	0.195	N/A

	Prior Years	FY 2019		FY 2020		FY 2021 Base		FY 2021 OCO		FY 2021 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	-	1.453		0.000		-		-		-	0.000	1.453	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2021 Air Force		Date: February 2020
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Enterprise (AF KME)*

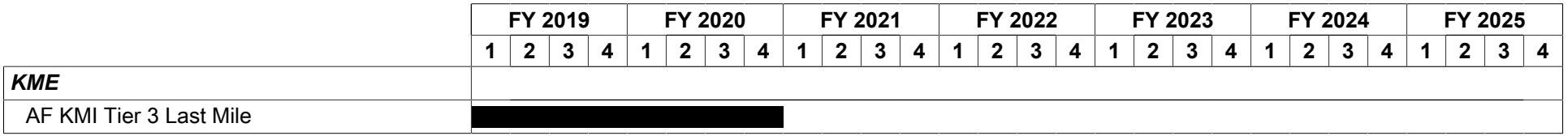

Exhibit R-4A, RDT&E Schedule Details: PB 2021 Air Force		Date: February 2020
Appropriation/Budget Activity 3600 / 7	**R-1 Program Element (Number/Name)** PE 0303140F / *Information Systems Security Program*	**Project (Number/Name)** 675231 / *AF Key Management Enterprise (AF KME)*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
KME				
AF KMI Tier 3 Last Mile	1	2019	4	2020