

UNCLASSIFIED

PE NUMBER: 0303140F
 PE TITLE: Information Systems Security Program

Exhibit R-2, RDT&E Budget Item Justification	DATE February 2008
---	------------------------------

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program
--	--

Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total
Total Program Element (PE) Cost	156.125	186.255	187.933	255.280	175.493	194.117	187.990	Continuing	TBD
4579 Adv Security Solutions & Technologies (ASST)	1.942	3.180	0.000	0.000	0.000	0.000	0.000	Continuing	TBD
4861 AF Electronic Key Management System (AF EKMS)	4.130	4.726	3.152	3.053	2.960	2.271	2.187	Continuing	TBD
5100 Cryptographic Modernization	139.500	167.832	172.038	239.337	159.498	178.558	172.243	Continuing	TBD
5231 AF Key Management Infrastructure (AF KMI)	0.691	4.378	5.239	5.217	5.244	5.346	5.455	Continuing	TBD
7820 Computer Security RDT&E: Firestarter	9.862	6.139	7.504	7.673	7.791	7.942	8.105	Continuing	TBD

NOTES:

1. In FY05, the Air Force funding for Project 674579, ASST, was terminated. However, it has continued to receive Congressional adds in FY05-FY08. Its Mission Statement has been revised annually to reflect the work of the current Congressional adds under the Project.

(U) A. Mission Description and Budget Item Justification

The overall focus of the RDT&E efforts within this program is two-fold. Focus one is to provide the capability to protect and defend USAF Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) and Weapon Systems from Information Warfare (IW) attacks and to ensure their recovery from such attacks. To this end, the project does research and development of information protection tools and transitions them to operational systems. Focus two is transforming electronic key delivery and DoD cryptographic devices to meet the next generation warfighting requirements. This includes: 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). Thus, eliminating the current key vulnerability to compromise by individuals transporting or loading key; and 2. a reduced inventory of cryptographic devices that are more robust, stronger, able to communicate extremely large amounts of data at greatly increased data rates, be upgraded more easily and less expensively, and are net-centric and Global Information Grid-compatible.

Project 674579, Advanced Security Solutions and Technologies, was originally established to develop defensive information warfare solutions for AF Command and Control (C2), Intelligence, Surveillance, and Reconnaissance (ISR) systems. The AF funding for the Project was terminated in FY05, but the funding line has continued with multiple Congressional adds in FY06-FY08. In FY08 it received two Congressional adds for Cybersecurity Defend and Attack Exercises. The first add is a continuation from previous years to provide funding for exercises in the local San Antonio, TX area. The second add funds an expansion effort to provide two community exercises in Montana. These adds are being managed by the Air Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) under the CIAS umbrella. They will bring a multi-disciplinary (AF, academic, and civil) approach to the planning and execution of joint military base/local civil agency Cybersecurity Defend and Attack Exercises.

Exhibit R-2, RDT&E Budget Item Justification

DATE

February 2008

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

0303140F Information Systems Security Program

Project 674861, AFEKMS, is part of an NSA-led DoD EKMS program that has allowed DoD to migrate from the previous legacy manual system of generation, distribution, accounting, training, and material management of cryptographic keying materials to the current DoD EKMS. EKMS equipment procurement and fielding is well underway. The R&D portion of the AFEKMS Program will support EKMS software upgrade, maintenance, and repair throughout the life of the next-generation system, KMI (Capability Increment 2 [CI-2]). The warfighter will continue to use EKMS for the next several years -- having access to it through the old EKMS hierarchy or through the new KMI hierarchy and its interfaces back to EKMS until the fielding of Capability Increment CI-3 KMI. The CI-3 KMI will replace all of the EKMS functions.

Project 675100, AF Crypto Modernization, is part of a Joint Program led by NSA to replace, modernize, and transform the Type 1 Cryptographic Inventory throughout DoD. Not only will algorithms be upgraded, but reprogrammable chips will be used in the Crypto Devices. Thus, the next generation of algorithm upgrades will incur only the cost to reprogram those chips. The total inventory will be greatly reduced by doing a box-for-family of systems/functions replacement rather than the current box-for-box replacement. The logistics requirements will also be greatly simplified and reduced. The total inventory and logistics requirements will be reduced by going to multi-purpose, Joint solution crypto devices instead of the current Service-unique inventories.

Project 675231, AF KMI, is part of another Joint Program led by NSA to provide a broad-scale replacement of the current EKMS. It will provide capabilities that will allow networked operation in consonance with the Global Information Grid (GIG) and DoD, other Service, and AF Enterprise objectives. KMI will improve protection of security-related information by greatly enhancing confidentiality, integrity, and non-repudiation beyond that provided by the legacy EKMS. It will take the man "out-of-the-loop" in the distribution of crypto key materials.

Project 677820, Computer Security RDT&E: Firestarter, encompasses the R&D of information protection technology and tools to defend C4ISR systems, with emphasis on computer and network systems security, damage assessment and recovery, and secure distributed computing capabilities. It provides access control, integrity, assured services that continue to meet the warfighters' requirements. Its products are flowed down into the existing operational Network Operations Security Centers (NOSCs) and all of the Base Infrastructure Protection Systems (BIPs).

This program is in budget activity 7, Operational System Development, because it addresses the development and transition of information security, protection and defensive capabilities and technologies.

Exhibit R-2, RDT&E Budget Item Justification

DATE

February 2008

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

0303140F Information Systems Security Program

(U) **B. Program Change Summary (\$ in Millions)**

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Previous President's Budget	184.610	229.657	194.981
(U) Current PBR/President's Budget	156.125	186.255	187.933
(U) Total Adjustments	-28.485	-43.402	
(U) Congressional Program Reductions	-15.000	-44.247	
Congressional Rescissions	-0.913	-1.555	
Congressional Increases	2.000	2.400	
Reprogrammings	-9.955		
SBIR/STTR Transfer	-4.617		

(U) **Significant Program Changes:**

The FY08 Appropriations Act Rescinded \$15M from the FY07 overall funding for AF RDT&E, ISSP.

The FY08 Appropriations Act also reduced BPAC 67510, AF Cryptographic Modernization, FY08 by \$45.047M for "unjustified program growth".

BPAC 674579, ASST, supports two Congressional adds in FY08: one for the on-going Cybersecurity Defend and Attack Exercise and one for the new Montana Cybersecurity Defend and Attack Exercise.

BPAC 675100, Cryptographic Modernization (CM), is a large umbrella capabilities-based AF program to support the overall NSA Cryptographic Modernization Initiative (CMI) to modernize and transform the current Type 1 Cryptographic Inventory throughout DoD. As such, it is composed of a sizeable number of individual cryptographic development programs that are staggered throughout the life of the AF CM Program. These development programs are centrally-managed, but decentrally-executed. The number of scheduled and on-going development programs varies from year-to-year leading to an unusual funding profile across the FYDP. However, detailed analysis of the requirements for the on-going development programs for any given year fully justifies the funding profile.

Exhibit R-2a, RDT&E Project Justification

DATE
February 2008

BUDGET ACTIVITY 07 Operational System Development				PE NUMBER AND TITLE 0303140F Information Systems Security Program			PROJECT NUMBER AND TITLE 4579 Adv Security Solutions & Technologies (ASST)		
Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total
4579 Adv Security Solutions & Technologies (ASST)	1.942	3.180	0.000	0.000	0.000	0.000	0.000	Continuing	TBD
Quantity of RDT&E Articles	0	0	0	0	0	0	0		

(U) A. Mission Description and Budget Item Justification

Project 674579, Advanced Security Solutions and Technologies, was originally established to develop defensive information warfare solutions for AF Command and Control (C2), Intelligence, Surveillance, and Reconnaissance (ISR) systems. The AF funding for Project 674579 was terminated in FY05. However, the Project remains active because of Congressional adds in FY05, FY06 and FY07. In FY08 the project line received two Congressional adds: one for the continuing Cybersecurity Defend and Attack Exercise in San Antonio, TX; another for an expansion of that effort to the Great Falls, MT location, entitled Montana Cybersecurity Defend and Attack Exercise.

The Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio (UTSA) has multiple funding sources, and is a multidisciplinary information assurance research and development, academic, and operationally-based program. It brings AF, academic, and civilian expertise to create a joint approach to technical and policy issues, civil threat information collection and reporting, as well as conducting joint military base/local civil agency Cybersecurity Defend and Attack Exercises. The aim of the work is to determine the degree of reliance of military establishments on locally-operated services, how military bases and posts currently participate in testing the local critical infrastructures, and how they would participate and respond to attacks to local critical infrastructure.

This project is in Budget Activity 7, Operational System Development, because it addresses the development and transition of information security, protection, and defensive capabilities and technologies.

(U) B. Accomplishments/Planned Program (\$ in Millions)

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Manage the Cybersecurity Defend and Attack Exercise (Congressional Add)	1.942	2.380	
(U) Manage the Montana Cybersecurity Defend and Attack Exercise (Congressional Add)		0.800	
(U) Total Cost	1.942	3.180	0.000

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

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Cost to</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Complete</u>	
(U) Other APPN									
N/A									

(U) D. Acquisition Strategy

Congressional adds are for a specific on-going effort being done for AFISRA under the Center for Infrastructure Assurance and Security Program (CIAS) at University

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

**0303140F Information Systems
Security Program**

PROJECT NUMBER AND TITLE

**4579 Adv Security Solutions &
Technologies (ASST)**

of Texas at San Antonio; and an extension of that effort to be conducted in Great Falls, MT. The extension effort will also be done for AFISRA by the CIAS Program.

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE				PROJECT NUMBER AND TITLE				
07 Operational System Development				0303140F Information Systems Security Program				4579 Adv Security Solutions & Technologies (ASST)				
(U) <u>Cost Categories</u> (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2007 Cost</u>	<u>FY 2007 Cost</u>	<u>FY 2007 Award Date</u>	<u>FY 2008 Cost</u>	<u>FY 2008 Award Date</u>	<u>FY 2009 Cost</u>	<u>FY 2009 Award Date</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
(U) <u>Product Development</u> Cybersecurity Defend and Attack Exercise (Congressional Add)	FY03 Information Warfare Broad Area Announcem ent (IW BAA) Grant Amendment	University of TX San Antonio, San Antonio, TX	2.100	1.942	Sep-07	2.380	Jan-08	0.000		0.000	6.422	TBD
Montana Cybersecurity Defend and Attack Exercises (Congressional Add)	FY03 Information Warfare Broad Area Announcem ent (IW BAA) Grant Amendment	FY03 Information Warfare Broad Area Announcement (IW BAA) Grant Amendment				0.800	Jan-08	0.000		0.000	0.800	TBD
Subtotal Product Development			2.100	1.942		3.180		0.000		0.000	7.222	TBD
Remarks:												
(U) Total Cost			2.100	1.942		3.180		0.000		0.000	7.222	TBD

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
4579 Adv Security Solutions & Technologies (ASST)

Exhibit R-4: BPAC 4579, ASST

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13							
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
Manage Cybersecurity Defend and Attack Exercise	█				█																											
Manage Montana Cybersecurity Defend and Attack Exercise																																

- ☆ Major Event or Milestone
- █ Planned Ongoing Activity
- █ Ongoing Activity that is Complete
- ▲ Completed Event
- △ Planned Task(s)

Exhibit R-4a, RDT&E Schedule Detail

DATE

February 2008

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE

4579 Adv Security Solutions & Technologies (ASST)

(U) Schedule Profile

FY 2007

FY 2008

FY 2009

(U) Manage the Cybersecurity Defend and Attack Exercise

1-4Q

1-4Q

(U) Manage the Montana Cybersecurity Defend and Attack Exercise

1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE
February 2008

BUDGET ACTIVITY 07 Operational System Development				PE NUMBER AND TITLE 0303140F Information Systems Security Program			PROJECT NUMBER AND TITLE 4861 AF Electronic Key Management System (AF EKMS)		
Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total
4861 AF Electronic Key Management System (AF EKMS)	4.130	4.726	3.152	3.053	2.960	2.271	2.187	Continuing	TBD
Quantity of RDT&E Articles	0	0	0	0	0	0	0		

NOTE:
Former Project 674861, AF Electronic Key Management System - Key Management Infrastructure (AFEKMS-KMI), was split in FY07 to properly reflect the Joint KMI Program as a next-generation system rather than an upgrade to the current EKMS. The AFEKMS stayed in BPAC 674861; the AF KMI moved to a new BPAC, 675231.

(U) A. Mission Description and Budget Item Justification

The AFEKMS Program consists of multiple developments supporting the Air Force requirements/portion of the DoD EKMS Program. (The National Security Agency [NSA] acts as the Executive Agency for the DoD EKMS Program.) AFEKMS, in concert with the overarching DoD EKMS Program, provides a secure and flexible capability for the electronic generation, distribution, accounting, and management of key material, voice callwords, and communications security (COMSEC) publications for the current generation of DoD Command, Control, Communications, Computers, and Intelligence (C4I) and for current generation of weapon systems. 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. AFEKMS has a three-tier hierarchical structure. This tiered structure provides 'wholesale' to 'retail' to 'consumer' capability to distribute, manage and account for COMSEC keying material. Tier 1 installations comprise the wholesale generation and control capability. Tier 2 installations comprise the local distribution network and Tier 3 comprises the retail where keying material leaves the AFEKMS and enters the consumer End Cryptographic Units (ECUs).

EKMS improved protection of national security-related information by substantially enhancing confidentiality, integrity, and non-repudiation characteristics over the legacy manual key management systems. EKMS has and continues to greatly accelerate availability of crypto key materials through electronic transmission 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 provide a temporary bridge to the DoD Key Management Infrastructure (KMI) Capability Increment (CI)-2, and then a migration path to the "full-up" KMI CI-3. Once KMI CI-3, with its advanced key generation/key distribution capability is fielded and operational, KMI interfaces to EKMS will be severed. Beginning KMI CI-2 functionality is expected in 2011.

This project is in Budget Activity 7, Operational System Development, because it addresses the development and transition of information security, protection, and defensive capabilities and technologies.

(U) B. Accomplishments/Planned Program (\$ in Millions)

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Continue program office contract support to the AFEKMS Program for planning: upgrade/improvements to the EKMS necessary to support the capabilities needed to bridge transition to the Key Management Infrastructure (KMI); EKMS continued deployment (Phase 5); interface and integration of key management into weapon systems; and tech refresh	0.863	1.180	1.478

UNCLASSIFIED

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 4861 AF Electronic Key Management System (AF EKMS)
---	---	---

(U) <u>B. Accomplishments/Planned Program (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Continue End User Application Software Development: Common User Application Software (CUAS), Data Management Device (DMD), and computer-based training	3.267	2.257	0.000
(U) Tier 2/3 Development: Support for ECU, weapon systems pending transition to KMI, and associated user software development		1.289	1.674
(U) Total Cost	4.130	4.726	3.152

(U) <u>C. Other Program Funding Summary (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Cost to</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Complete</u>	
(U) AF Other Procurement PE 0303140F	12.270	10.539	12.521	21.094	21.199	21.613	22.040	Continuing	TBD

Note: This line includes both AFEKMS and AF KMI Other Procurement (3080) funding.

(U) **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.

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE					PROJECT NUMBER AND TITLE				
07 Operational System Development				0303140F Information Systems Security Program					4861 AF Electronic Key Management System (AF EKMS)				
<u>(U) Cost Categories</u> (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2007 Cost</u>	<u>FY 2007 Cost</u>	<u>FY 2007 Award Date</u>	<u>FY 2008 Cost</u>	<u>FY 2008 Award Date</u>	<u>FY 2009 Cost</u>	<u>FY 2009 Award Date</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>	
<u>(U) Product Development</u>													
AFEKMS Program office contractor support for planning	CPFF	Mitre, San Antonio, TX	3.804	0.863	Jan-07	1.237	Jan-08	1.431	Jan-09	Continuing	TBD	TBD	
End User Application Software Development	T&M	SAIC, San Diego, CA	11.669	3.267	Jan-07	2.000	Jan-08	0.000			16.936	16.936	
Tier 2/3 Development	TBD	TBD	0.000	0.000		1.489	Jan-08	1.721	Jan-09	Continuing	TBD	TBD	
Subtotal Product Development			15.473	4.130		4.726		3.152		Continuing	TBD	TBD	
Remarks:													
<u>(U) N/A</u>													
<u>(U) Total Cost</u>			15.473	4.130		4.726		3.152		Continuing	TBD	TBD	
Remarks:	N/A												

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
4861 AF Electronic Key Management System (AF EKMS)

Exhibit R-4: BPAC 4861, AFEKMS

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
AFEKMS Program office contractor support for planning and migration to the KMI Infrastructure				▲	<i>Phase 5 Pilot</i>																							
End User Application Software Development: CUAS, DMDs, & computer-based training					<i>CUAS 5.1</i> ☆							☆	<i>CUAS 5.2</i>															
Tier 2/3 Development																												

Notes:

1. Pilot – Consists of 8 COMSEC Accounts which will be converted to connect to the KMI Tiers above it via IP over SUPRNet rather than the current method using STU II/IIIs over the Public Switched Network (PSN)
2. CUAS – Common User Application Software

☆ Major Event or Milestone

▬ Planned Ongoing Activity

▬ Ongoing Activity that is Complete

▲ Completed Event

△ Planned Task(s)

Exhibit R-4a, RDT&E Schedule Detail

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 4861 AF Electronic Key Management System (AF EKMS)
---	---	---

(U) <u>Schedule Profile</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) AFEKMS Program office contractor support for planning	1-4Q	1-4Q	1-4Q
(U) Phase 5 Pilot	4Q		
(U) End User Application Software Development	1-4Q	1-4Q	1-3Q
(U) CUAS 5.1 Rollout		3Q	
(U) CUAS 5.2 Rollout			3Q
(U) Tier 2/3 Development		3-4Q	1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY		PE NUMBER AND TITLE					PROJECT NUMBER AND TITLE			
07 Operational System Development		0303140F Information Systems Security Program					5100 Cryptographic Modernization			
Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total	
5100 Cryptographic Modernization	139.500	167.832	172.038	239.337	159.498	178.558	172.243	Continuing	TBD	
Quantity of RDT&E Articles	0	0	0	0	0	0	0			

(U) A. Mission Description and Budget Item Justification

(U) The Cryptographic Modernization Program modernizes cryptographic devices protecting critical information vital to successful mission operations and national security. In September 2000, the Defense Review Board (DRB) tasked NSA to evaluate the security posture of the cryptographic inventory. Systems with aging algorithms, those approaching non-sustainability, and those generally incompatible with modern key management systems were identified. Priority systems that required immediate replacement were also identified. In addition, NSA documented the need to modernize the cryptographic inventory with capabilities designed to enable network-centric operations. Replacements/Modernization of the near term vulnerable systems must occur within the timeframe specified in Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. The DoD Cryptographic Modernization Program was established to develop a modern cryptographic base that provides assured security robustness, interoperability, advanced algorithms, releasability, programmability, and compatibility with the future Key Management Infrastructure (KMI). The program supports the transformation 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 IAW national and international policy/standards, the validated operational requirements of the warfighters, and the Intelligence Communities.

(U) The Cryptographic Modernization Program is a collection of projects accomplished in three phases: Replacement, Modernization, and Transformation. The Replacement Phase of the program focused on updating and/or replacing out-of-date algorithms along with unsustainable cryptographic products. The Modernization Phase provides a common solution to existing multiple 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 network-centric capabilities and seamless crypto that is transparent to the user.

(U) This project is in Budget Activity 07, Operation System Development, because it addresses the development and transition of information security, protection, and defensive capabilities and technologies.

(U) B. Accomplishments/Planned Program (\$ in Millions)

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Completed KS-60 (KI-22) Cryptographic Modernization analysis and development of replacement	19.477	0.000	0.000
(U) Continue KG-3X Cryptographic Modernization development and test efforts of replacement crypto devices	10.435	24.543	30.744
(U) Continue IFF Cryptographic Modernization analysis and development of replacement	13.022	12.416	0.000
(U) Continue F-22 Multi-Function Crypto (Crypto Mod of KOV-20 & generic KOV-xx boxes)	3.789	1.138	5.780
(U) Continue Remote Rekey (CI-13) Cryptographic Modernization	3.071	9.700	18.303
(U) Continue Studies and Analyses (includes Crypto Transformation Initiative)	20.864	37.381	21.969
(U) Continue Space Cryptographic Modernization (includes Space Telemetry tracking and Commanding project and	42.226	37.001	49.832

R-1 Line Item No. 165

Page-14 of 33

Project 5100

Exhibit R-2a (PE 0303140F)

Exhibit R-2a, RDT&E Project Justification

DATE
February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 5100 Cryptographic Modernization
--	--	--

(U) B. Accomplishments/Planned Program (\$ in Millions)	FY 2007	FY 2008	FY 2009
Space Mission Data project)			
(U) Merged Wireless Cryptographic Modernization analysis with KMEM	0.200	0.000	0.000
(U) Merged KM Crypto Interface Modernization analyses with KMEM	1.284	0.000	0.000
(U) Merged KM Network Equipment Modernization analyses with KMEM	0.369	0.000	0.000
(U) Continue KM Equipment Modernization (KMEM) development	0.000	5.449	4.893
(U) Broke out KEESEE Cryptographic Modernization analysis (broken out into the following five individual Crypto Mod development programs after FY07)	15.647	0.000	0.000
(U) Continue KOK-13 Combat Key Generator (formerly known as the earlier CM initiative KOK-13 Key Generation Modernization under KEESEE)	0.000	12.029	10.676
(U) Continue VINSON/ANDVT Cryptographic Modernization (VACM) (formerly known as Secure Data Link Crypto under KEESEE)	0.000	3.529	11.970
(U) Continue Link 16 Encryption Modernization (LSEM)) (formerly known as Secure Data Link Crypto under KEESEE)	0.000	0.306	6.777
(U) Continue Range Telemetry Encryption Modernization (RTEM) (formerly known as Secure Data Link Crypto under KEESEE)	0.000	0.798	0.000
(U) Continue Secure Crypto Enterprise Management (SCEM) (formerly known as Secure Data Link Crypto under KEESEE)	0.000	0.112	1.333
(U) Merged High Speed Crypto analysis with Advanced Common Crypto	0.200	0.000	0.000
(U) Continue Advanced Crypto Modernization analysis and development (includes Smart Munitions, High Speed Crypto and Programmanble Objective Encryption Technologies [POET] [formerly know as Common Engines/Modules])	8.916	23.430	9.761
(U) Total Cost	139.500	167.832	172.038

(U) C. Other Program Funding Summary (\$ in Millions)	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Cost to Complete</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>		
(U) AF Other Procurement PE 0303140F	48.434	56.603	44.885	77.221	143.041	217.821	266.739	Continuing	TBD

(U) D. Acquisition Strategy
The Crypto Modernization portfolio of component and system acquisition projects are executing using a variety of approaches that vary from an evolutionary acquisition strategy using spiral development (for new system 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.

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 5100 Cryptographic Modernization
--	--	--

<u>(U) Cost Categories</u> (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2007 Cost</u>	<u>FY 2007 Cost</u>	<u>FY 2007 Award Date</u>	<u>FY 2008 Cost</u>	<u>FY 2008 Award Date</u>	<u>FY 2009 Cost</u>	<u>FY 2009 Award Date</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
(U) <u>Product Development</u> KS-60 (KI-22)	MIPRed to OO-ALC 526 GSSG. OO-ALC put on a CPAF contract.	OO-ALC/526 GSSG/GMGV, Hill AFB, UT	52.895	19.477	Jan-07	0.000		0.000		0.000	72.372	72.372
KG-3X	MIPRed to 639th ELSS/KM. ESC puts on a CPAF contract	6939th ELSS/KM, Hanscom AFB, MA	8.617	10.435	Jan-07	24.543	Jan-08	30.744	Jan-09	0.000	74.339	39.392
IFF	CPSG puts on two CPFF contracts.	CPSG/ZC, Lackland AFB, TX	30.750	13.022	Jan-07	12.416	Jan-08	0.000		0.000	56.188	47.888
F-22/ Multi Function Crypto (KOV -20)	MIPRed to ASC/YF. ASC puts two separate CPFF delivery orders to an existing CNI 2010 FFP contract.	ASC/YFAA F-22 SPO, Wright Patterson AFB, OH	0.000	3.789	Feb-07	1.138	Feb-08	5.780	Feb-09	Continuing	TBD	TBD
Remote Rekey	CPSG will put on a TBD Contract.	CPSG/ZC, Lackland AFB, TX	3.345	3.071	Jan-07	9.700	Jan-08	18.303	Jan-09	Continuing	TBD	TBD
Studies and Analyses	CPSG puts on three T&M contracts.	CPSG/ZX, Lackland AFB, TX	39.268	20.864	Jan-07	37.381	Jan-08	21.969	Jan-09	Continuing	TBD	TBD
Space Crypto Mod	CPSG puts	CPSG/ZJ,	27.045	42.226	Jan-07	37.001	Jan-08	49.832	Jan-09	Continuing	TBD	TBD

R-1 Line Item No. 165

Page-16 of 33

Project 5100

Exhibit R-3 (PE 0303140F)

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis										DATE February 2008		
BUDGET ACTIVITY 07 Operational System Development				PE NUMBER AND TITLE 0303140F Information Systems Security Program				PROJECT NUMBER AND TITLE 5100 Cryptographic Modernization				
Wireless Cryptographic Modernization analysis	on a CPFF contract. TBD	Lackland AFB, TX TBD	0.000	0.200	Feb-07	0.000	0.000	0.000	0.200	0.200	0.000	
KM Crypto Interface Modernization analyses	MIPRed to Fr. Monmouth, NJ for FFP Contract.	SNC, Sparks, NC	0.000	1.284	Feb-07	0.000	0.000	0.000	1.284	TBD	0.000	
KM Network Equipment Modernization analyses	CAT I MIPR to NRL, DC; CAT II MIPR to Ft. Monmouth, NJ; CAT II MIPR to Hill AFB, UT	NRL, Washington, DC; BAH, San Antonio, TX; 309 NXW, Hill AFB, UT	0.000	0.369		0.000	0.000	0.000	0.369	TBD	0.000	
KM Equipment Modernization development	CPSG placed on a T&M Contract	CPSG/NI, Lackland AFB, TX	0.000	0.000		5.449	Feb-08	4.893	Feb-09	Continuing	TBD	TBD
KEESEEE Cryptographic Modernization analysis (broken out into the following five individual Crypto Mod development programs after FY07)			11.026	15.647	Feb-07	0.000	0.000	0.000	26.673	8.382	0.000	
KOK-13 Combat Key Generator (formerly known as the earlier CM initiative, KOK-13 Key Generation Modernization) *	TBD	TBD	0.000	0.000		12.029	Feb-08	10.676	Feb-09	0.000	22.705	6.886
VINSON/ANDVT Cryptographic Modernization (formerly known as Secure Voice)	TBD	TBD	0.000	0.000		3.529	Feb-08	11.970	Feb-09	Continuing	TBD	TBD
Link 16 Encryption Modernization (formerly known as Secure Data Link)	TBD	TBD	0.000	0.000		0.306	Feb-08	6.777	Feb-09	Continuing	TBD	TBD
Range Encryption Modernization (former known as Telemetry Analyses and Development of Replacements)	TBD	TBD	0.000	0.000		0.798	Feb-08	0.000	Feb-09	Continuing	TBD	TBD

R-1 Line Item No. 165

Page-17 of 33

Project 5100

Exhibit R-3 (PE 0303140F)

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE				PROJECT NUMBER AND TITLE				
07 Operational System Development				0303140F Information Systems Security Program				5100 Cryptographic Modernization				
Secure Crypto Enterprise Management (SCEM)	TBD	TBD	0.000	0.000	0.112	Feb-08	1.333	Feb-09	Continuing	0.000	TBD	TBD
High Speed Crypto analysis	TBD	TBD	0.000	0.200	Feb-07	0.000	0.000	0.000	0.000	0.200	0.200	
Advanced Common Crypto Modernization analysis and development (includes High Speed Optical Crypto, Common Crypto Engines/Modules, and Smart Munitions)	TBD	TBD	0.000	8.916	Feb-07	23.430	Feb-08	9.761	Feb-09	Continuing	TBD	TBD
Subtotal Product Development			172.946	139.500		167.832		172.038	Continuing	0.000	TBD	TBD
Remarks:	* NOTE: Early efforts within the AF CM Program to scope requirements, determine work needed to provide modernization and/or transformation solutions, consider viable solutions, etc. are considered "in-house efforts" and labeled "CM Initiatives". If no requirements are found or work already underway will provide a solution, the initiative is closed out. Some initiatives will point to a common solution, and be merged to form and initiate a new CM project. For some initiatives, individual solutions will be able to be crafted within on-going projects, and the work under the initiative will be dispersed across on-going or newly initiated projects.											
(U) Total Cost			172.946	139.500		167.832		172.038	Continuing	TBD	TBD	

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
5100 Cryptographic Modernization

Exhibit R-4: BPAC 5100 Cryptographic Modernization (p 1 of 3)

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
KS-60			▲		MS C																							
KG-3X*									☆	MS C																		
IFF						★	MS C																					
F-22 Multi-Function Crypto Modernization																												
Remote Rekey (CI-13)						★	MS H								☆	MS C												
Studies and Analyses (includes CTI)**																												
Space CM (Space TT&C)		▲			MS B GOE Inc 1			☆				☆			☆		MS B AVE/GOE Inc 2											
Space CM (Space Mission Data)					★	MS B Inc 1			MS C GOE Inc 1		MS C AVE Inc 1				MS C Inc 1	☆							☆	MS B Inc 2				

MS C AVE/GOE Inc 2 ☆
MS C Inc 2 - TBD ☆

- ☆ Major Event or Milestone
- ▬ Planned Ongoing Activity
- ▬ Ongoing Activity that is Complete
- Planned Combining/Splitting of Program
- ▲ Completed Event
- △ Planned Task(s)

* Schedule reflects the new KG-3X program revised baseline.
** Studies and Analyses includes KMI Transformation

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
5100 Cryptographic Modernization

Exhibit R-4: BPAC 5100 Cryptographic Modernization (p 2 of 3)

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Wireless Cryptographic Mod Analysis (merged with KMEM)	█				█																							
KM Crypto Interface Modernization (merged with KMEM)	█				█																							
KM Network Equipment Modernization (merged with KMEM)	█				█																							
KM Equipment Modernization (KMEM)					█				☆ MS B								☆ MS C											
KEESEE (split into the next 5 individual programs)	█				█																							
Combat Key Generator-CKG (formerly KOK-13 Modernization)	█				█				☆ MS B				☆ MS C															
Vinson-ANDVT (formerly Secure Voice Project)	█				█				☆ MS B				☆ MS C															

- ☆ Major Event or Milestone
- █ Planned Ongoing Activity
- █ Ongoing Activity that is Complete
- Planned Combining/Splitting of Program
- ▲ Completed Event
- △ Planned Task(s)

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
5100 Cryptographic Modernization

Exhibit R-4: BPAC 5100 Cryptographic Modernization (p 3 of 3)

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13							
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
Link-16 Encryption Modernization (LSEM) Crypto																																
Range Telemetry Encryption Modernization (RTEM)***																																
Secure Crypto Enterprise Management (SCEM)																																
High Speed Crypto (Merged with Advanced Common Crypto)																																
Advanced Common Crypto Modernization (Smart Munitions) ****																																
Advanced Common Crypto Modernization (High Speed Crypto)																																
Advanced Common Crypto Modernization (POET)																																

Split from KE ESEE

3

4

5



- ☆ Major Event or Milestone
- ▬ Planned Ongoing Activity
- ▬ Ongoing Activity that is Complete
- ➔ Planned Combining/Splitting of Program
- ▲ Completed Event
- △ Planned Task(s)

*** RTEM revised acquisition strategy pending
**** Smart Munitions Increment 2 milestones TBD

MS B Inc 2-TBD



UNCLASSIFIED

Exhibit R-4a, RDT&E Schedule Detail

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 5100 Cryptographic Modernization
--	--	--

(U) Schedule Profile	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Completed KS-60 (KI-22) Cryptographic Modernization	1-4Q	1Q	
(U) Continue KG-3X Cryptographic Modernization*	1-4Q	1-4Q	
(U) Complete IFF Mode 5 Cryptographic Modernization	1-4Q	1-4Q	
(U) Continue F/A-22 Multi Function Crypto (Crypto Mod of KOV-20 & generic KOV-xx boxes)	1-4Q	1-4Q	1-4Q
(U) Continue Remote Rekey (CI-13) Cryptographic Modernization	1-4Q	1-4Q	1-4Q
(U) Continue Studies and Analyses (includes Crypto Transformation Initiative)	1-4Q	1-4Q	1-4Q
(U) Continue Space Cryptographic Modernization (includes Space Telemetry Tracking and Commanding project and the Space Mission Data project)	1-4Q	1-4Q	1-4Q
(U) Wireless Cryptographic Modernization analyses (merged with KMEM)	1-2Q		
(U) KM Network Equipment Modernization analyses (merged with KMEM)	1-4Q		
(U) KM Network Interface Modernization analyses (merged with KMEM)	1-2Q		
(U) Continue KM Equipment Modernization (KMEM) Development		1-4Q	1-4Q
(U) KEESEE Cryptographic Modernization analysis broken out into the following five individual Crypto Mod development programs after FY07)	1-4Q		
(U) Continue KOK-13 Combat Key Generator (formerly known as the earlier CM initiative KOK-13 Key Generation Modernization under KEESEE)	1-4Q	1-4Q	1-4Q
(U) Continue Link 16 Encryption Modernization (LSEM) (formerly known as Secure Data Link Crypto under KEESEE)		1-4Q	1-4Q
(U) Continue Range Telemetry Encryption Modernization (RTEM) (formerly known as Secure Data Link Crypto under KEESEE)		1-4Q	
(U) Continue Secure Crypto Enterprise Management (SCEM) (formerly known as Secure Data Link Crypto under KEESEE)		1-4Q	1-4Q
(U) High Speed Optical Crypto analysis (merged with Advanced Common Crypto)	1-4Q		
(U) Continue Advanced Common Crypto Modernization analysis and development (includes High Speed Optical Cryp, Common Crypto Engines/Modules, and Smart Munitions)	1-4Q	1-4Q	1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development				PE NUMBER AND TITLE 0303140F Information Systems Security Program			PROJECT NUMBER AND TITLE 5231 AF Key Management Infrastructure (AF KMI)		
Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total
5231 AF Key Management Infrastructure (AF KMI)	0.691	4.378	5.239	5.217	5.244	5.346	5.455	Continuing	TBD
Quantity of RDT&E Articles	0	0	0	0	0	0	0		

NOTE:

Former Project 674861, AF Electronic Key Management System - Key Management Infrastructure (AFEKMS-KMI) was split in FY07 to properly reflect the Joint KMI Program as a next-generation system rather than an upgrade to the current EKMS. The AFEKMS stayed in BPAC 674861; the AF KMI moved to this new BPAC, 675231. However, since the transformational key generation/key provisioning capability will not be built into KMI until Capability Increment (CI)-3, EKMS will continue to provide this capability via a number of temporary interfaces created for that purpose.

(U) **A. Mission Description and Budget Item Justification**

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

The AF Key Management Infrastructure (KMI) Program's R&D efforts will include: building the AF KMI architecture; defining all of its linkages; building the linkage interfaces that will allow them to communicate; and other "last mile" development. (See NOTE below for detailed explanation of the "last mile" work.)

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 key management system. KMI will greatly accelerate the availability of crypto key materials through electronic transmission versus shipping of materials, will enhance mission responsiveness and flexibility, and will take the man "out-of-the-loop" in the distribution of crypto key materials.

This project is in Budget Activity 7, Operational System Development, because it addresses the development and transition of information security, protection, and defensive capabilities and technologies.

NOTE: In parallel, DoD and the Services are developing a new generation of End Crypto Units (ECUs) under the Joint Crypto Modernization Initiative that will be capable of direct interaction with the KMI. (See BPAC 675100, this PE, for the AF CM Program supporting 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) keying material from a KMI client to a new generation ECU will need to be handled in the early years by one of two data transfer devices. CPSG and NSA are exploring new key delivery methods for KMI CI-3: "Mobile" COMSEC Accounts that can be wheeled out to platforms and remote ECUs; a new Simple Key Loader (SKL) for Special Operations that carries more

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 5231 AF Key Management Infrastructure (AF KMI)
---	---	---

keys and is smaller and lighter; and a method called "over-the-air-keying (OTAK)" to ultimately replace the data transfer devices.

(U) <u>B. Accomplishments/Planned Program (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Provide program office contract support for Air Force Key Management planning and systems integration, and migration to the Key Management Infrastructure	0.691	1.560	2.089
(U) Develop the next generation Last Mile Systems & Concept Refinement (F22): End user key delivery devices; user node application software; and related computer-based training	0.000	2.818	3.150
(U) Total Cost	0.691	4.378	5.239

(U) <u>C. Other Program Funding Summary (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Cost to</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Complete</u>	
(U) See AF Other Procurement PE 33140F	12.270	10.593	12.521	21.094	21.199	21.631	22.040	Continuing	TBD

Note: this line includes both AFEKMS and AF KMI Other Procurement (3080) money.

(U) **D. Acquisition Strategy**
 All major contracts within this Project are awarded after full and open competition.

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE					PROJECT NUMBER AND TITLE				
07 Operational System Development				0303140F Information Systems Security Program					5231 AF Key Management Infrastructure (AF KMI)				
(U) <u>Cost Categories</u> (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2007 Cost</u>	<u>FY 2007 Cost</u>	<u>FY 2007 Award Date</u>	<u>FY 2008 Cost</u>	<u>FY 2008 Award Date</u>	<u>FY 2009 Cost</u>	<u>FY 2009 Award Date</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>	
(U) <u>Product Development</u>													
Architectural Planning & Migration (to) the KMI Infrastructure Studies & Analyses & Systems Engineering	CPFF	MITRE, San Antonio, TX	0.000	0.691	Jan-07	0.873	Jan-08	0.911	Jan-09	Continuing	TBD	TBD	
Last Mile Development	CPFF	TBD	0.000	0.000		2.574	Jan-08	3.160	Jan-09	Continuing	TBD	TBD	
Subtotal Product Development			0.000	0.691		4.133		4.980		Continuing	TBD	TBD	
Remarks:													
(U) <u>Support</u>													
Budget Analyst	T&M	BAH, San Antonio, TX	0.000	0.000		0.125	Mar-08	0.134	Mar-09	Continuing	TBD	TBD	
System Administrator						0.120	Jul-08	0.125	Jul-09	Continuing	TBD	TBD	
Subtotal Support			0.000	0.000		0.245		0.259		Continuing	TBD	TBD	
Remarks:													
(U) <u>Test & Evaluation</u>													
Subtotal Test & Evaluation			0.000	0.000		0.000		0.000			0.000	0.000	
Remarks:													
(U) <u>Management</u>													
Subtotal Management			0.000	0.000		0.000		0.000			0.000	0.000	
Remarks:													
(U) Total Cost			0.000	0.691		4.378		5.239		Continuing	TBD	TBD	

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
5231 AF Key Management Infrastructure (AF KMI)

Exhibit R-4: BPAC 5321, AF KMI

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13							
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
Architectural Planning & Migration (to) the KMI Infrastructure																	☆				KMI CA-2				MS C							
Last Mile Development & Concept Refinement (F-22). (Expedited, Secure Delivery of crypto key from the Local COMSEC Accounts to its ECUs)																																

- ☆ Major Event or Milestone
- ▬ Planned Ongoing Activity
- ▬ Ongoing Activity that is Complete
- ▲ Completed Event
- △ Planned Task(s)

UNCLASSIFIED

Exhibit R-4a, RDT&E Schedule Detail	DATE February 2008
--	------------------------------

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 5231 AF Key Management Infrastructure (AF KMI)
--	--	--

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Schedule Profile			
(U) Architectural Planning & Migration (to) the KMI Infrastructure	1-4Q	1-4Q	1-4Q
(U) Develop next generation Last Mile Systems & Concept Refinement (F-22)		1-4Q	1-4Q
(U) MS B			3Q

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE			PROJECT NUMBER AND TITLE		
07 Operational System Development				0303140F Information Systems Security Program			7820 Computer Security RDT&E: Firestarter		
Cost (\$ in Millions)	FY 2007 Actual	FY 2008 Estimate	FY 2009 Estimate	FY 2010 Estimate	FY 2011 Estimate	FY 2012 Estimate	FY 2013 Estimate	Cost to Complete	Total
7820 Computer Security RDT&E: Firestarter	9.862	6.139	7.504	7.673	7.791	7.942	8.105	Continuing	TBD
Quantity of RDT&E Articles	0	0	0	0	0	0	0		

(U) **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 protect and defend Air Force Network-Centric Command, Control, Communications, Computer, and Intelligence (C4I) systems from computer network attacks, and ensure recovery from those attacks. As one of the Air Force managers for IA R&D, the PMO ensures that the emphasis of the program is directed toward information/computer/network security; damage assessment and recovery; dynamic security policy enforcement; and active response and attribution. These areas of emphasis are realized through cyberspace surveillance; cyber indications and warning (CI&W); high-speed and host-based intrusion detection; fusion and correlation of attack indicators; decision support; recovery; cyber forensics; and active response. Current Air Force systems, such as the Combat Information Transport System/Base Information Protection (CITS/BIP) and Information Warfare Planning Capability (IWPC), leverage this technology to meet their information protection needs/requirements. Additionally, this program utilizes IA technology investments by the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), Department of National Intelligence (DNI), Disruptive Technology Office (DTO), and the Department of Homeland Security (DHS), Advanced Research Project Activity (ARPA) to jump-start its development of solutions to existing Air Force IA requirements. This program coordinates and cooperates with the JTF-GNO, STRATCOM, DISA, NSA and other services to ensure Global Information Grid (GIG) IA requirements are being met.

This program is in Budget Activity 7, Operational System Development, because it addresses the development and transition of information security, protection, and defensive capabilities and technologies.

(U) **B. Accomplishments/Planned Program (\$ in Millions)**

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Completed development of secure agent frameworks for Enterprise Defense to support protection of the warfighter C4ISR systems	0.750	0.000	0.000
(U) Completed IP v6 Risk Mitigation	0.454	0.000	0.000
(U) Continue development of cyber forensic tools and methodologies	0.908	0.320	0.282
(U) Continue development of technology for self-healing, self-regenerative systems (to include automated system recovery)	0.950	0.670	0.830
(U) Continue development of information attack correlation methodologies	0.800	0.768	0.680
(U) Completed development of methodologies for Steganography Detection and Dynamic Quarantine of Worms	0.523	0.408	0.000
(U) Continue effort to transition DARPA/DTO/ARPA information assurance (IA) technology into AF Information Protection, Detection, & Response architecture	0.810	0.616	0.660
(U) Continue effort to develop metrics for reliable information assurance (IA) measurement and testing	0.350	0.276	0.303
(U) Continue development of secure interoperable distributed agent computing	0.975	0.475	0.588

R-1 Line Item No. 165

Page-28 of 33

Project 7820

Exhibit R-2a (PE 0303140F)

Exhibit R-2a, RDT&E Project Justification

DATE

February 2008

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 7820 Computer Security RDT&E: Firestarter
---	---	--

(U) <u>B. Accomplishments/Planned Program (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Continue effort to provide active response, dynamic policy Enforcement and computer/network attack attribution	0.787	0.617	0.724
(U) Continue effort to provide dynamic, cost effective, risk mitigation information assurance techniques for wireless networks and systems	0.547	0.330	0.557
(U) Continue effort to provide IA/Cyber modeling and simulation for mission impact assessment and dynamic network security planning	0.686	0.260	0.572
(U) Continue effort to provide secure coalition IA data management, collaboration, and visualization	0.675	0.415	0.684
(U) Completed effort to provide Internet Protocol (IP) Telephony (Voice Over IP) security tools	0.444	0.000	0.000
(U) Continue Cyber Security Bots	0.203	0.417	0.832
(U) Continue Integrated Airborne Network Security IO Platform	0.000	0.567	0.792
(U) Total Cost	9.862	6.139	7.504

(U) <u>C. Other Program Funding Summary (\$ in Millions)</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Cost to</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Estimate</u>	<u>Complete</u>	
(U) Other APPN N/A									

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

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE

February 2008

BUDGET ACTIVITY				PE NUMBER AND TITLE					PROJECT NUMBER AND TITLE			
07 Operational System Development				0303140F Information Systems Security Program					7820 Computer Security RDT&E: Firestarter			
<u>(U) Cost Categories</u> (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2007 Cost</u>	<u>FY 2007 Cost</u>	<u>FY 2007 Award Date</u>	<u>FY 2008 Cost</u>	<u>FY 2008 Award Date</u>	<u>FY 2009 Cost</u>	<u>FY 2009 Award Date</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
(U) <u>Product Development</u> FFRDC (MITRE)	CPFF	Multiple Locations	6.304	0.558	Jan-07	0.370	Jan-08	0.396	Jan-09	Continuing	TBD	TBD
Multiple Contractors	CPFF	Multiple Locations	97.664	8.004	Jan-07	4.969	Jan-08	6.263	Jan-09	Continuing	TBD	TBD
Multiple Universities	CPFF	Multiple Locations	14.816	1.300	Jan-07	0.800	Jan-08	0.845	Jan-09	Continuing	TBD	TBD
Subtotal Product Development			118.784	9.862		6.139		7.504		Continuing	TBD	TBD
Remarks:	Multiple contractors & multiple universities reflect on-going efforts with over a dozen contractors & universities. Each has a different contract date depending on when that particular contract was awarded.											
(U) Total Cost			118.784	9.862		6.139		7.504		Continuing	TBD	TBD

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2008

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303140F Information Systems Security Program

PROJECT NUMBER AND TITLE
7820 Computer Security RDT&E: Firestarter

Exhibit R-4: BPAC 7820, Firestarter (p 1 of 2)

Fiscal Year	FY 07				FY 08				FY 09				FY 10				FY 11				FY 12				FY 13			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Requirements Review Board		▲				△				△				△				△				△				△		
Secure Agent Frameworks for Enterprise Defense	■	■	■	▲																								
IP v6 Risk Mitigation	■	■	■	▲																								
CyberForensic Tools & Methodologies	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Self-healing, Self-regenerative Systems			▲						△				△								△							
Information Attack Correlation Methodologies			▲								△										△							
Steganography Detection & Dynamic Quarantine of Worms	■	■	■	■	■	■	■	■	△																			
Transition of new DARPA/DTO/ARPA IA technologies	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Metrics for IA Measurement & Testing											△												△					
Secure Interoperable Distributed Agent Computing	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

△

- ☆ Major Event or Milestone
- Planned Ongoing Activity
- Ongoing Activity that is Complete
- ▲ Completed Event
- △ Planned Task(s)

UNCLASSIFIED

Exhibit R-4a, RDT&E Schedule Detail	DATE February 2008
--	------------------------------

BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303140F Information Systems Security Program	PROJECT NUMBER AND TITLE 7820 Computer Security RDT&E: Firestarter
--	--	---

	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Schedule Profile			
(U) Requirements Review Boards	2Q	2Q	2Q
(U) Completed development of secure agent frameworks for Enterprise Defense	1-4Q		
(U) Completed IPv6 Risk Mitigation	1-4Q		
(U) Continue development of cyber forensic tools and methodologies	1-4Q	1-4Q	1-4Q
(U) Continue development of technology for self-healing, self-regenerative systems	1-4Q	1-4Q	1-4Q
(U) Continue information attack correlation methodologies	1-4Q	1-4Q	1-4Q
(U) Completed development of methodologies for steganography detection and dynamic quarantine of worms	1-4Q		
(U) Continue DARPA/ DTO/ARPA information assurance Technology transition	1-4Q	1-4Q	1-4Q
(U) Continue to develop metrics for reliable IA measurement and testing	1-4Q	1-4Q	1-4Q
(U) Continue secure interoperable distributed agent computing (partial Congressional add)	1-4Q	1-4Q	1-4Q
(U) Continue to develop active response, dynamic policy enforcement, and computer/network attack attribution	1-4Q	1-4Q	1-4Q
(U) Continue risk mitigation IA techniques for wireless networks and systems	1-4Q	1-4Q	1-4Q
(U) Continue IA/Cyber modeling and simulation for mission impact assessment and dynamic network security planning	1-4Q	1-4Q	1-4Q
(U) Continue secure coalition IA data management collaboration and visualization	1-4Q	1-4Q	1-4Q
(U) Completed Internet Protocol (IP) Telephony (Voice Over IP) security tools	1-4Q		
(U) Continue Cyber Security Bots (Cybercraft)	4Q	1-4Q	1-4Q
(U) Continue Integrated Airborne Network Security IO platform		1-4Q	1-4Q