

UNCLASSIFIED

PE NUMBER: 0303140F

PE TITLE: Information Systems Security Program

Exhibit R-2, RDT&E Budget Item Justification	DATE February 2007
---	------------------------------

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

Cost (\$ in Millions)	FY 2006 Actual	FY 2007 Estimate	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	103.288	184.610	229.657	194.981	264.302	183.898	202.868	196.816	Continuing	TBD
4579 Adv Security Solutions & Technologies (ASST)	4.100	1.992	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	TBD
4861 AF Electronic Key Management System (AF EKMS)	3.273	2.331	4.767	3.178	3.082	2.989	2.293	2.208	Continuing	TBD
5100 Cryptographic Modernization	86.871	173.868	214.285	178.955	248.207	167.748	187.158	180.917	Continuing	TBD
5231 AF Key Management Infrastructure (AF KMI)	0.000	0.709	4.415	5.282	5.267	5.295	5.398	5.508	0.000	0.000
7820 Computer Security RDT&E: Firestarter	9.044	5.710	6.190	7.566	7.746	7.866	8.019	8.183	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, FY06, and FY07. Its Mission Statement has been revised annually to reflect the work of the current Congressional adds under the Project.
2. Former Project 674861, AF Electronic Key Management System - Key Management Infrastructure (AFEKMS-KMI), was split in FY07 to properly reflect the DoD KMI Program as a next-generation system rather than an upgrade to the current DoD EKMS. The AFEKMS stayed in BPAC 674861; the AF KMI moved to the new BPAC 675231.

(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 continued that year with two Congressional adds -- as well as in FY06 with three Congressional adds: the Center for Infrastructure Assurance and Security (CIAS), Cybersecurity Defend and Attack Exercises, and Homeland Defense and Civil Support Threat Information Collection. In FY07 it received only one Congressional add for the Cybersecurity Defend and Attack Exercises. These adds are being managed by the Air Intelligence Agency (AIA) under the CIAS umbrella. They will

Exhibit R-2, RDT&E Budget Item Justification

DATE

February 2007

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

0303140F Information Systems Security Program

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.

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 fielded Capability Increment (CI-2) KMI. 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. 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, and the logistics requirements will be greatly simplified and reduced. The total inventory and logistics requirements are also 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. In FY06 this project received a Congressional add of \$5M to support its on-going development of secure interoperable distributed agent computing (aka Worldwide Infrastructure Security Environment [WISE]).

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 2007

BUDGET ACTIVITY

07 Operational System Development

PE NUMBER AND TITLE

0303140F Information Systems Security Program

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

	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Previous President's Budget	116.532	183.523	319.016	201.193
(U) Current PBR/President's Budget	103.288	184.610	229.657	194.981
(U) Total Adjustments	-13.244			
(U) Congressional Program Reductions	0.000	-0.212		
Congressional Rescissions		-0.701		
Congressional Increases		2.000		
Reprogrammings	-10.003			
SBIR/STTR Transfer	-3.241			

(U) **Significant Program Changes:**

BPAC 674579, ASST, supports one Congressional add in FY07 Execution: the Cybersecurity Defend and Attack Exercises.

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.

BPAC 675100, Cryptographic Modernization (CM) FY08: Funding reduced to support higher DoD priorities.

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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 2006 Actual	FY 2007 Estimate	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)	4.100	1.992	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	TBD
Quantity of RDT&E Articles	0	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 FY06 the project line received three Congressional adds: Center for Infrastructure Assurance and Security (CIAS), Cybersecurity Defend and Attack Exercises, and Homeland Defense and Civil Support Threat Information Collection. All three FY06 plus-ups are being managed by Air Intelligence Agency (AIA) under the CIAS umbrella. In FY07 the project line received only on Congressional add for the Cybersecurity Defend and Attack Exercises.

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 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Managed the Center for Infrastructure Assurance and Security (CIAS) (Congressional Add)	1.000	0.000	0.000	0.000
(U) Managed the Homeland Defense and Civil Support Threat Information Collection (Congressional Add)	1.000	0.000	0.000	0.000
(U) Manage the Cybersecurity Defend and Attack Exercises (Congressional Add)	2.100	1.992	0.000	0.000
(U) Total Cost	4.100	1.992	0.000	0.000

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

	<u>FY 2006</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>Complete</u>							
(U) Other APPN										
N/A										

Exhibit R-2a, RDT&E Project Justification

DATE

February 2007

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) D. Acquisition Strategy

Congressional adds are for specific efforts to be done for AIA under the Center for Infrastructure Assurance and Security Program (CIAS) at either University of Texas at San Antonio or St. Mary's University in San Antonio.

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis

DATE
February 2007

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) <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 2006 Cost</u>	<u>FY 2006</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2009</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
				<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>			
(U) <u>Product Development</u> Center for Infrastructure Assurance and Security (CIAS) Projects (Congressional Add)	FY03 Informatio n Warfare Broad Area Announce ment (IW BAA) Grant Amendme nt	University of TX San Antonio, San Antonio, TX	7.782	1.000	Sep-06	0.000		0.000		0.000		0.000	8.782	8.782
Homeland Defense and Civil Support Threat Information Collection (Congressional Add)	FY03 Informatio n Warfare Broad Area Announce ment (IW BAA) Grant Amendme nt	St. Mary's University, San Antonio, TX	0.000	1.000	Sep-06	0.000		0.000		0.000		0.000	1.000	1.000
Cybersecurity Defend and Attack Exercises (Congressional Add)	FY03 Informatio n Warfare Broad Area Announce ment (IW BAA) Grant Amendme nt	University of TX San Antonio, San Antonio, TX	0.000	2.100	Sep-06	1.992	Sep-07	0.000		0.000		0.000	4.092	TBD
Subtotal Product Development			7.782	4.100		1.992		0.000		0.000		0.000	13.874	TBD
Remarks:														
(U) Total Cost			7.782	4.100		1.992		0.000		0.000		0.000	13.874	TBD

Exhibit R-4, RDT&E Schedule Profile

DATE
February 2007

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 06				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	1	2	3	4
Manage CIAS Congressional Add)	█																															
Manage Homeland Defense and Civil Support Threat Information Collection (Congressional Add)	█																															
Manage Cybersecurity Defend and Attack Exercised (Congressional Add)	█				█																											

- ☆ 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 2007

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

- (U) Managed the Center for Infrastructure Assurance and Security (CIAS)
- (U) Managed the Homeland Defense and Civil Support Threat Information Collection
- (U) Managed the Cybersecurity Defend and Attack Exercises

FY 2006

FY 2007

FY 2008

FY 2009

1-4Q

1-4Q

1-4Q

1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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 2006 Actual	FY 2007 Estimate	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)	3.273	2.331	4.767	3.178	3.082	2.989	2.293	2.208	Continuing	TBD	
Quantity of RDT&E Articles	0	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 2009.

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)

	FY 2006	FY 2007	FY 2008	FY 2009
(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	1.286	0.860	1.777	1.015

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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 2006</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	1.987	1.471	1.368	0.000
(U) Tier 2/3 Development: Support for ECU and weapon systems pending transition to KMI	0.000	0.000	1.622	2.163
(U) Total Cost	3.273	2.331	4.767	3.178

(U) <u>C. Other Program Funding Summary (\$ in Millions)</u>	<u>FY 2006</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>Complete</u>							
(U) AF Other Procurement PE 0303140F	15.844	12.270	11.149	12.606	21.264	21.382	21.801	22.233	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 2007

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>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 2006 Cost</u>	<u>FY 2006</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2009</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
				<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>	<u>Cost</u>	<u>Award</u>			
(U) <u>Product Development</u>														
AFEKMS Program office contractor support for planning	CPFF	Mitre, San Antonio, TX	2.518	1.286	Jan-06	0.860	Jan-07	1.777	Jan-08	1.015	Jan-09	Continuing	TBD	TBD
End User Application Software Development	T&M	SAIC, San Diego, CA	9.682	1.987	Jan-06	1.471	Jan-07	1.368	Jan-08	0.000			14.508	14.508
Tier 2/3 Development	TBD	TBD	0.000	0.000		0.000		1.622	Jan-08	2.163	Jan-09	Continuing	TBD	TBD
Subtotal Product Development			12.200	3.273		2.331		4.767		3.178		Continuing	TBD	TBD
Remarks:														
(U) <u>N/A</u>														
(U) Total Cost			12.200	3.273		2.331		4.767		3.178		Continuing	TBD	TBD
Remarks:	N/A													

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2007

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 06				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	1	2	3	4				
AFEKMS Program office contractor support for planning and migration to the KMI Infrastructure				▲			△		<i>Phase 5 Pilot</i>																											
	<i>Phase 5 IATO *</i>																																			
End User Application Software Development: CUAS, DMDs, & computer-based training																																				
	 <i>CUAS 5.0</i> <i>CUAS 5.1</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 SIPNet rather than the current method using STU II's/III's over the Public Switched Network (PSN)
2. IATO – Initial Authority to Operate
3. CUAS – Common User Application Software
4. DMDs – Data Management Devices

☆ 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 2007
--	------------------------------

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>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) <u>Schedule Profile</u>				
(U) AFEKMS Program office contractor support for planning	1-4Q	1-4Q	1-4Q	1-4Q
(U) Phase 5 IATO	4Q			
(U) Phase 5 Pilot		3Q		
(U) End User Application Software Development	1-4Q	1-4Q	1-4Q	
(U) CUAS 5.0 Rollout		3Q		
(U) CUAS 5.1 Rollout			2Q	
(U) Tier 2/3 Development			2Q	1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

BUDGET ACTIVITY 07 Operational System Development					PE NUMBER AND TITLE 0303140F Information Systems Security Program			PROJECT NUMBER AND TITLE 5100 Cryptographic Modernization		
Cost (\$ in Millions)	FY 2006 Actual	FY 2007 Estimate	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	86.871	173.868	214.285	178.955	248.207	167.748	187.158	180.917	Continuing	TBD
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0		

(U) A. Mission Description and Budget Item Justification

The Cryptographic Modernization Program modernizes vulnerable 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. 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.

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 as identified in the Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. The Modernization Phase provides a single solution to existing multiple cryptographic end items, as well as updating mid-term aging/unsupportable crypto equipment identified in the Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. Logistics requirements begin to 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 solutions which enable network-centric capabilities and seamless crypto that is transparent to the user.

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 2006</u>	<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	20.953	19.477	0.000	0.000
(U) Complete KG-3X Cryptographic Modernization analysis and development of replacement	6.745	10.765	20.010	0.000
(U) Complete IFF Cryptographic Modernization analysis and development of replacement	9.208	13.276	3.862	0.000
(U) Continue FA-22 Multi-Function Crypto (KOV-20) Cryptographic Modernization analysis and development	0.000	5.507	15.507	11.501
(U) Continue Remote Rekey (CI-13) Cryptographic Modernization analysis and development of replacement	3.345	9.950	19.417	14.667
(U) Continue Studies and Analyses	18.378	25.283	19.693	16.826

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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)	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Continue Space Cryptographic Modernization analyses and development of replacements	17.216	44.560	57.024	47.149
(U) Wireless Cryptographic Modernization analysis	0.000	0.200	0.000	0.000
(U) KM Crypto Interface Modernization analyses	0.000	1.284	0.000	0.000
(U) KM Network Equipment Modernization analyses	0.000	0.200	0.000	0.000
(U) KM Equipment Modernization development	0.000	0.000	6.050	4.403
(U) KEESEE Cryptographic Modernization analysis (broken out into the following five individual Crypto Mod development programs after FY07)	11.026	35.022	0.000	0.000
(U) Initiate KOK-13 Combat Key Generator (formerly known as the earlier CM initiative KOK-13 Key Generation Modernization)	0.000	0.000	10.677	9.077
(U) Initiate Secure Voice Project (includes Secure Voice Transitional Development and an Enhanced Airborne STE)	0.000	0.000	14.517	34.075
(U) Initiate Secure Data Link Crypto (includes Miniaturization and Crypto Modernized Waveforms [for example, JTIDS-Link 16], and KG-13A [for EPLRS/SADL])	0.000	0.000	28.990	24.296
(U) Initiate Telemetry Analyses and Development of Replacements	0.000	0.000	4.938	12.908
(U) Initiate Secure Crypto Enterprise Management (SCEM)	0.000	0.000	1.200	0.200
(U) High Speed Optical Crypto analysis	0.000	0.200	0.000	0.000
(U) Continue Advanced Cryptographic Modernization analysis and development (includes High Speed Optical Crypto, Common Crypto Engines/Modules, and Smart Munitions)	0.000	8.144	12.400	3.853
(U) Total Cost	86.871	173.868	214.285	178.955

(U) C. Other Program Funding Summary (\$ in Millions)	<u>FY 2006</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 Complete</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</u>								
(U) AF Other Procurement PE 0303140F	0.000	56.994	115.234	157.983	199.795	261.362	266.481	271.768	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 2007

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 2006 Cost</u>	<u>FY 2006 Cost</u>	<u>FY 2006 Award Date</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/UT V, Hill AFB, UT	31.942	20.953	Jan-06	19.477	Jan-07	0.000		0.000		0.000	72.372	72.372
KG-3X	MIPRed to ESC/GIG SG/KM. ESC puts on a CPAF contract.	ESC/GIGSG/KM, Hanscom AFB, MA	1.872	6.745	Jan-06	10.765	Jan-07	20.010	Jan-08	0.000		0.000	39.392	39.392
IFF	MIPRed to CPSG/ZC. CPSG puts on two CPFF contracts.	CPSG/ZC, Lackland AFB, TX	21.542	9.208	Jan-06	13.276	Jan-07	3.862	Jan-08	0.000		0.000	47.888	47.888
F/A-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	0.000	Jan-06	5.507	Feb-07	15.507	Feb-08	11.501	Feb-09	Continuing	TBD	TBD

R-1 Line Item No. 174

Page-16 of 33

Project 5100

Exhibit R-3 (PE 0303140F)

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis											DATE			
											February 2007			
BUDGET ACTIVITY				PE NUMBER AND TITLE				PROJECT NUMBER AND TITLE						
07 Operational System Development				0303140F Information Systems Security Program				5100 Cryptographic Modernization						
Remote Rekey (CI-13)	MIPRed to CPSG/CZ. CPSG will put on a TBD Contract.	CPSG/ZC, Lackland AFB, TX	0.000	3.345	Jan-06	9.950	Jan-07	19.417	Jan-08	14.667	Jan-09	Continuing	TBD	TBD
Studies and Analyses	MIPRed to CPSG/CZ. CPSG puts on three T&M contracts.	CPSG/ZC, Lackland AFB, TX	20.890	18.378	Jan-06	25.283	Jan-07	19.693	Jan-08	16.826	Jan-09	Continuing	TBD	TBD
Space Crypto Mod	MIPRed to CPSG/CZ. CPSG puts on a CPEFF contract.	CPSG/ZC, Lackland AFB, TX	9.829	17.216	Jan-06	44.560	Jan-07	57.024	Jan-08	47.149	Jan-09	Continuing	TBD	TBD
Wireless Cryptographic Modernization analysis	TBD	TBD	0.000	0.000		0.200	Feb-07	0.000		0.000		0.000	0.200	0.200
KM Crypto Interface Modernization analyses	TBD	TBD	0.000	0.000		1.284	Feb-07	0.000		0.000		0.000	1.284	TBD
KM Network Equipment Modernization analyses	TBD	TBD	0.000	0.000		0.200	Feb-07	0.000		0.000		0.000	0.200	TBD
KM Equipment Modernization development	TBD	TBD	0.000	0.000		0.000		6.050	Feb-08	4.403	Feb-09	Continuing	TBD	TBD
KEESEEE Cryptographic Modernization analysis (broken out into the following five individual Crypto Mod development programs after FY07)			0.000	11.026	Feb-06	35.022	Feb-07	0.000		0.000		0.000	46.048	8.382
KOK-13 Combat Key Generator (formerly known as the earlier CM initiative, KOK-13 Key Generation Modernization) *	TBD	TBD	0.000	0.000		0.000		10.677	Feb-08	9.077	Feb-09	0.000	19.754	6.886
Secure Voice Project (includes Secure Voice	TBD	TBD	0.000	0.000		0.000		14.517	Feb-08	34.075	Feb-09	Continuing	TBD	TBD

R-1 Line Item No. 174

Page-17 of 33

Project 5100

Exhibit R-3 (PE 0303140F)

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2007

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 06				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	1	2	3	4				
Wireless Cryptographic Mod Analysis Split & Merged with two others					█	█	█	█																												
KME Equipment Modernization	█	█	█	█	█	█	█	█	☆ MSB								☆ MSC																			
KEESEE Analyses (being rolled out to individual projects starting in FY08)	█	█	█	█	█	█	█	█																												
KEESEE Analyses: Combat Key Generator (KOK-13 Modernization)					☆ MSB								☆ MSC																							
KEESEE Analyses: Secure Voice									MSB ☆								☆ MSC																			
KEESEE Analyses: Secure Tactical Comm																					☆ MSB	☆ LEF			☆ MSC	☆ LEF			☆				☆ MSC	☆ HAIFE		

- ☆ 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 2007

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 06				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	1	2	3	4
KS-60	█				█				☆ MS C																							
KG-3X	█				█				█				☆ MS C								Transformation - P3.L for KMI											
IFF Mode 5 CM	█				█				☆ MS C												Competibility ☆ MS B											
F-22 Multi-Function Crypto Modernization					█				█				█				█				█				█							
Remote Rekey (CI-13)	█				█				☆ MS B								☆ MS C															
Studies and Analyses	█				█				█				█				█				█				█							
Space CM	★ MS B AVE		█		★ MS B GCE		█						☆ MS C AVE		█		█		█		█		█		█		█		█			

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

UNCLASSIFIED

Exhibit R-4a, RDT&E Schedule Detail		DATE February 2007		
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 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Completed KS -60 (KI-22) Cryptographic Modernization	1-4Q	1-3Q		
(U) Complete KG-3X Cryptographic Modernization	1-4Q	1-4Q	1-4Q	
(U) Continue IFF Mode 5 Cryptographic Modernization	1-4Q	1-4Q	1-2Q	
(U) Continue F/A-22 Multi Function Crypto (Crypto Mod of KOV-20 Box)		1-4Q	1-4Q	1-4Q
(U) Continue Remote Rekey (CI-13) Cryptographic Modernization	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue Studies and Analyses	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue Space Cryptographic Modernization	1-4Q	1-4Q	1-4Q	1-4Q
(U) Wireless Cryptographic Modernization analyses		1-4Q		
(U) KM Network Interface Modernization analyses		1-4Q		
(U) KM Equipment Modernization 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	1-4Q		
(U) Initiate/Complete KOK-13 Combat Key Generator (formerly known as the earlier CM initiative KOK-13 Key Generation Modernization) *			1-4Q	1-4Q
(U) Initiate Secure Voice Project (includes Secure Voice Transitional Development and an Enhanced Airborne STE)			1-4Q	1-4Q
(U) Initiate Secure Data Link Crypto (includes Miniaturization, and Crypto Modernized Waveforms [for example, JTIDS-Link 16], and KG-13A [for EPLRS/SADL])			1-4Q	1-4Q
(U) Initiate Telemetry Analyses and Replacement Developments			1-4Q	1-4Q
(U) Initiate Secure Crypto Enterprise Management (SCEM)			1-4Q	1-4Q
(U) High Speed Optical Crypto analysis		1-4Q		
(U) Continue Advanced Cryptographic Modernization analysis and development (includes High Speed Optical Crypto, Common Crypto Engines/Modules, and Smart Munitions)		1-4Q	1-4Q	1-4Q

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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 2006 Actual	FY 2007 Estimate	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)	0.000	0.709	4.415	5.282	5.267	5.295	5.398	5.508	0.000	0.000
Quantity of RDT&E Articles	0	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

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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)
---	---	---

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

(U) B. Accomplishments/Planned Program (\$ in Millions)	<u>FY 2006</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	0.000	0.709	1.553	2.460
(U) Develop the next generation Last Mile Systems: End user key delivery devices; user node application software; and related computer-based training	0.000	0.000	2.862	2.822
(U) Total Cost	0.000	0.709	4.415	5.282

(U) C. Other Program Funding Summary (\$ in Millions)	<u>FY 2006</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>Complete</u>							
(U) See AF Other Procurement PE 33140F	15.844	12.270	11.149	12.606	21.264	21.382	21.801	22.233	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 2007

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) Cost Categories (Tailor to WBS, or System/Item Requirements) (\$ in Millions)	<u>Contract Method & Type</u>	<u>Performing Activity & Location</u>	<u>Total Prior to FY 2006 Cost</u>	<u>FY 2006 Cost</u>	<u>FY 2006 Award Date</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	CPFF	MITRE, San Antonio, TX	0.000	0.000		0.709	Jan-07	1.553	Jan-08	2.460	Jan-09	Continuing	TBD	TBD
Last Mile Development	CPFF	TBD	0.000	0.000		0.000		2.862	Jan-08	2.822	Jan-09	Continuing	TBD	TBD
Subtotal Product Development			0.000	0.000		0.709		4.415		5.282		Continuing	TBD	TBD
Remarks:														
(U) <u>Support</u>													0.000	0.000
Subtotal Support			0.000	0.000		0.000		0.000		0.000		0.000	0.000	0.000
Remarks:														
(U) <u>Test & Evaluation</u>													0.000	0.000
Subtotal Test & Evaluation			0.000	0.000		0.000		0.000		0.000		0.000	0.000	0.000
Remarks:														
(U) <u>Management</u>													0.000	0.000
Subtotal Management			0.000	0.000		0.000		0.000		0.000		0.000	0.000	0.000
Remarks:														
(U) Total Cost			0.000	0.000		0.709		4.415		5.282		Continuing	TBD	TBD

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2007

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

CI-3 CDD	FY 06				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	1	2	3	4				
Architectural Planning & Migration (to) the KMI Infrastructure								△	<i>CI-3 CDD</i>																											
Last Mile Development (Expedited, Secure Delivery of crypto key from the Local COMSEC Accounts to its ECUs)								☆												☆																
									<i>MS B</i>																											
									<i>MS C</i>																											

- ☆ 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 2007

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) Schedule Profile

(U) Architectural Planning & Migration (to) the KMI Infrastructure

(U) CI-3 CDD

(U) Develop next generation Last Mile Systems

(U) MS B

FY 2006

FY 2007

FY 2008

FY 2009

1-4Q

1-4Q

1-4Q

4Q

1-4Q

1-4Q

1Q

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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			
Cost (\$ in Millions)	FY 2006 Actual	FY 2007 Estimate	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	9.044	5.710	6.190	7.566	7.746	7.866	8.019	8.183	Continuing	TBD	
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0			

(U) A. Mission Description and Budget Item Justification

The Firestarter program provides research and development (R&D) 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 2006</u>	<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	0.310	0.544	0.000	0.000
(U) Completed IP v6 Risk Mitigation	0.195	0.204	0.000	0.000
(U) Complete development of cyber forensic tools and methodologies	0.278	0.408	0.320	0.000
(U) Continue development of technology for self-healing, self-regenerative systems (to include automated system recovery)	0.458	0.624	0.670	0.830
(U) Continue development of information attack correlation methodologies	0.602	0.662	0.768	0.630
(U) Continue development of methodologies for Steganography Detection and Dynamic Quarantine of Worms	0.122	0.188	0.408	0.522
(U) Continue effort to transition DARPA/DTO/ARPA information assurance (IA) technology into AF Information Protection, Detection, & Response architecture	0.254	0.449	0.616	0.660

Exhibit R-2a, RDT&E Project Justification

DATE
February 2007

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) B. Accomplishments/Planned Program (\$ in Millions)	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Continue effort to develop metrics for reliable information assurance (IA) measurement and testing	0.136	0.159	0.276	0.290
(U) Continue development of secure interoperable distributed agent computing (including FY06 Congressional Add for Worldwide Infrastructure Security Environment [WISE])	5.510	0.501	0.526	0.650
(U) Continue effort to provide active response, dynamic policy Enforcement and computer/network attack attribution	0.324	0.487	0.617	0.624
(U) Continue effort to provide dynamic, cost effective, risk mitigation information assurance techniques for wireless networks and systems	0.266	0.347	0.330	0.457
(U) Continue effort to provide IA/Cyber modeling and simulation for mission impact assessment and dynamic network security planning	0.210	0.271	0.260	0.472
(U) Continue effort to provide secure coalition IA data management, collaboration, and visualization	0.327	0.391	0.415	0.584
(U) Continue effort to provide Internet Protocol (IP) Telephony (Voice Over IP) security tools	0.052	0.272	0.280	0.333
(U) Continue Cyber Security Bots (Cybercraft)	0.000	0.203	0.417	0.832
(U) Initiate Integrated Airborne Network Security IO Platform	0.000	0.000	0.287	0.682
(U) Total Cost	9.044	5.710	6.190	7.566

(U) C. Other Program Funding Summary (\$ in Millions)	<u>FY 2006</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 Complete</u>	<u>Total Cost</u>
	<u>Actual</u>	<u>Estimate</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 2007

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>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 2006 Cost</u>	<u>FY 2006</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2009</u>	<u>Cost to Complete</u>	<u>Total Cost</u>	<u>Target Value of Contract</u>
				<u>Cost</u>	<u>Award Date</u>									
(U) <u>Product Development</u> FFRDC (MITRE)	CPFF	Multiple Locations		0.304	Jan-06	0.323	Jan-07	0.370	Jan-08	0.396	Jan-09	Continuing	TBD	TBD
Multiple Contractors	CPFF	Multiple Locations		8.184	Jan-06	4.674	Jan-07	5.020	Jan-08	6.325	Jan-09	Continuing	TBD	TBD
Multiple Universities	CPFF	Multiple Locations		0.556	Jan-06	0.713	Jan-07	0.800	Jan-08	0.845	Jan-09	Continuing	TBD	TBD
Subtotal Product Development			0.000	9.044		5.710		6.190		7.566		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			0.000	9.044		5.710		6.190		7.566		Continuing	TBD	TBD

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2007

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 06				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	1	2	3	4
Requirements Review Board		▲					△				△				△				△				△				△				△	
Secure Agent Frameworks for Enterprise Defense	■	■	■	■	■	■	■	■																								
IP v6 Risk Mitigation	■	■	■	■	■	■	■	■																								
Cyber Forensic Tools & Methodologies	■	■	■	■	■	■	■	■				△																				
Self-healing, Self-regenerative Systems	■	■	■	■	■	■	■	■			△			△				△						△								
Information Attack Correlation Methodologies	■	■	■	■	■	■	■	■			△					△																
Steganography Detection & Dynamic Quantization of Worms	■	▲	■	■	■	■	■	■								△																
Transition of new DARPA/DTO/ARPA IA technologies	■	■	■	■	■	■	■	■																								
Metrics for IA Measurement & Testin	■	■	■	■	■	■	■	■																								
Secure Interoperable Distributed Agent Computing (WISE)	■	▲	■	■	■	■	■	■			△																				△	

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

Exhibit R-4, RDT&E Schedule Profile

DATE

February 2007

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 2 of 2)

Fiscal Year	FY 06				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	1	2	3	4
Active Response, dynamic Policy Enforcement & Computer/Network Attack Attribution								△				△								△				△								
Risk Mitigation IA Techniques for Wireless																																
IA/Cyber M&S for Impact Assessment & Network Security Planning			▲					△								△																
Secure Coalition IA Data Mgmt., Collaboration, & Visualization								△				△								△												
IP Telephony (Voice over IP) security tools		▲														△																
Cyber Security Bots (Cybercraft)												△				△								△								
Integrated Airborne Network Security Platform												△				△								△								△

- ☆ 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 2007
--	------------------------------

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>Schedule Profile</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>
(U) Requirements Review Boards	2Q	2Q	2Q	2Q
(U) Completed development of secure agent frameworks for Enterprise Defense	1-4Q	1-4Q		
(U) Completed IPv6 Risk Mitigation	1-4Q	1-4Q		
(U) Complete 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	1-4Q
(U) Continue information attack correlation methodologies	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue development of methodologies for steganography detection and dynamic quarantine of worms	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue DARPA/ DTO/ARPA information assurance Technology transition	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue to develop metrics for reliable IA measurement and testing	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue secure interoperable distributed agent computing (partial Congressional add)	1-4Q	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	1-4Q
(U) Continue risk mitigation IA techniques for wireless networks and systems	1-4Q	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	1-4Q
(U) Continue secure coalition IA data management collaboration and visualization	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue Internet Protocol (IP) Telephony (Voice Over IP) security tools	1-4Q	1-4Q	1-4Q	1-4Q
(U) Continue Cyber Security Bots (Cybercraft)		3-4Q	1-4Q	1-4Q
(U) Initiate Integrated Airborne Network Security IO platform			2-4Q	1-4Q