PE NUMBER: 0303401F
PE TITLE: Communications Security

Exhibit R-2, RDT&E Budget Item Justification

DATE **February 2004**

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303401F Communications Security

Cost ($ in Millions)	FY 2003 Actual	FY 2004 Estimate	FY 2005 Estimate	FY 2006 Estimate	FY 2007 Estimate	FY 2008 Estimate	FY 2009 Estimate	Cost to Complete	Total
Total Program Element (PE) Cost	4.344	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	TBD
4861 Cryptologic 2000	4.344	0.000	0.000	0.000	0.000	0.000	0.000	Continuing	TBD

Note: Starting in FY04 this BPAC has been moved out of PE 33401F, Communications Security, and into PE 33140F, Information Systems Security Program (ISSP), with the same BPAC number and name.

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

The Cryptologic 2000 Project consists of multiple developments supporting the Air Force Electronic Key Management Systems (AFEKMS). AFEKMS, in concert with the National Security Agency's (NSA) EKMS, 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 AF Command, Control, Communications, Computers, and Intelligence (C4I) systems and weapon systems. AFEKMS replaces the existing physical distribution and management system providing cryptographic keying material for USAF Information Assurance. Information Assurance emphasizes access control, multi-level secure databases, trusted computing and information integrity. AFEKMS is a three-tier system structure in a hierarchical arrangement. 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' capability. Tier 2 installations comprise the distribution network and Tier 3 comprises the 'retail' locations where keying material leaves the AFEKMS and enters the End Item COMSEC Equipment (EICE).

Acquisition includes Commercial Off-The-Shelf (COTS) computers and software, contractor-developed application software, and Government Furnished Equipment (GFE) and software such as NSA's Local COMSEC Management Software (LCMS). The USAF-developed user application software (UAS) is necessary to provide a common framework for specific functions of unique key management systems such as the F-22, Advanced Extremely High Frequncy (EHF) COMSEC/TRANSEC System (ACTS), Joint Strike Fighter, and other current and future programs. Further, unique key fill requirements of EICE for AF applications such as ARC-210, Fighter Data Link, Airborne Integrated Terminal Group and Multi-Band Multi-Mode Radio, and other current and future programs are also supported by AFEKMS developments. The UASs developed by the AFEKMS System Program Office (SPO) improve the LCMS user interface, integrate multiple independent UASs into a single commonly supported package, and moderate unique UASs running on the same platform when integration is not possible. They also allow automation of manual operator processes in order to save manpower, reduce required training, and improve mission effectiveness.

Overall AFEKMS will improve protection of national security-related information by enhancing confidentiality, integrity, and non-repudiation substantially over legacy key management systems. AFEKMS will greatly accelerate availability of key through electronic transmission vice shipping of materials, and will enhance mission responsiveness and flexibility. While much of the current AFEKMS level of effort is directed at enhancing current and developing systems, the ultimate aim is to provide a migration path to future functionality planned under NSA's Key Management Infrastructure (KMI) initiative. Such KMI functionality is expected to emerge about 2007.

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 2004

BUDGET ACTIVITY
07 Operational System Development

PE NUMBER AND TITLE
0303401F Communications Security

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

		FY 2003	FY 2004	FY 2005
(U)	Previous President's Budget	4.765	0.000	0.000
(U)	Current PBR/President's Budget	4.344	0.000	0.000
(U)	Total Adjustments	-0.421	0.000	
(U)	Congressional Program Reductions	-0.006	0.000	
	Congressional Rescissions	-0.051	0.000	
	Congressional Increases	0.000	0.000	
	Reprogrammings	-0.093	0.000	
	SBIR/STTR Transfer	-0.271	0.000	

(U) Significant Program Changes:

Moved out of PE 0303401F, Communications Security, starting in FY04. Has been placed in PE 0303140F, Information Systems Security Program (ISSP), using the same Project number and BPAC name.

Exhibit R-2a, RDT&E Project Justification

DATE **February 2004**

BUDGET ACTIVITY **07 Operational System Development**

PE NUMBER AND TITLE **0303401F Communications Security**

PROJECT NUMBER AND TITLE **4861 Cryptologic 2000**

Cost ($ in Millions)	FY 2003 Actual	FY 2004 Estimate	FY 2005 Estimate	FY 2006 Estimate	FY 2007 Estimate	FY 2008 Estimate	FY 2009 Estimate	Cost to Complete	Total
4861 Cryptologic 2000	4.344	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		

(U) A. Mission Description and Budget Item Justification

The Cryptologic 2000 Project consists of multiple developments supporting the Air Force Electronic Key Management Systems (AFEKMS). AFEKMS, in concert with the National Security Agency's (NSA) EKMS, 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 AF Command, Control, Communications, Computers, and Intelligence (C4I) systems and weapon systems. AFEKMS replaces the existing physical distribution and management system providing cryptographic keying material for USAF Information Assurance. Information Assurance emphasizes access control, multi-level secure databases, trusted computing and information integrity. AFEKMS is a three-tier system structure in a hierarchical arrangement. 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' capability. Tier 2 installations comprise the distribution network and Tier 3 comprises the 'retail' locations where keying material leaves the AFEKMS and enters the End Item COMSEC Equipment (EICE).

Acquisition includes Commercial Off-The-Shelf (COTS) computers and software, contractor-developed application software, and Government Furnished Equipment (GFE) and software such as NSA's Local COMSEC Management Software (LCMS). The USAF-developed user application software (UAS) is necessary to provide a common framework for specific functions of unique key management systems such as the F-22, Advanced Extremely High Frequncy (EHF) COMSEC/TRANSEC System (ACTS), Joint Strike Fighter, and other current and future programs. Further, unique key fill requirements of EICE for AF applications such as ARC-210, Fighter Data Link, Airborne Integrated Terminal Group and Multi-Band Multi-Mode Radio, and other current and future programs are also supported by AFEKMS developments. The UASs developed by the AFEKMS System Program Office (SPO) improve the LCMS user interface, integrate multiple independent UASs into a single commonly supported package, and moderate unique UASs running on the same platform when integration is not possible. They also allow automation of manual operator processes in order to save manpower, reduce required training, and improve mission effectiveness.

Overall AFEKMS will improve protection of national security-related information by enhancing confidentiality, integrity, and non-repudiation substantially over legacy key management systems. AFEKMS will greatly accelerate availability of key through electronic transmission vice shipping of materials, and will enhance mission responsiveness and flexibility. While much of the current AFEKMS level of effort is directed at enhancing current and developing systems, the ultimate aim is to provide a migration path to future functionality planned under NSA's Key Management Infrastructure (KMI) initiative. Such KMI functionality is expected to emerge about 2007.

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)	FY 2003	FY 2004	FY 2005
(U) Continued program office contract support of EKMS User Application Software including migration to the Key Management Infrastructure (KMI) and the Browser-Based Development effort	1.347		

Exhibit R-2a, RDT&E Project Justification		DATE February 2004
BUDGET ACTIVITY 07 Operational System Development	PE NUMBER AND TITLE 0303401F Communications Security	PROJECT NUMBER AND TITLE 4861 Cryptologic 2000

(U)	Continued End User Application Software Development: common UAS, Local Management Device/Data Management Device (LMD/DMD) browser interface, KOV-21 Integration, and computer-based training	2.997		
(U)	Total Cost	4.344	0.000	0.000

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

		FY 2003 Actual	FY 2004 Estimate	FY 2005 Estimate	FY 2006 Estimate	FY 2007 Estimate	FY 2008 Estimate	FY 2009 Estimate	Cost to Complete	Total Cost
(U)	F-22 Engineering and Manufacturing Development (EMD) (BA05, PE 0604239F, Avionics Block 3.1.1)	1.300	0.000	0.000	0.000	0.000	0.000	0.000	0.000	3.000
(U)	Information Systems Security Program (ISSP) (Continuation of Project 674861under BA07, PE 030140F)	0.000	9.708	2.813	3.302	3.533	3.597	3.637	Continuing	TBD

(U) D. Acquisition Strategy

All major contracts within this Program Element were awarded after full and open competition.

Exhibit R-3, RDT&E Project Cost Analysis

DATE **February 2004**

BUDGET ACTIVITY **07 Operational System Development**

PE NUMBER AND TITLE **0303401F Communications Security**

PROJECT NUMBER AND TITLE **4861 Cryptologic 2000**

(U) Cost Categories (Tailor to WBS, or System/Item Requirements) ($ in Millions)	Contract Method & Type	Performing Activity & Location	Total Prior to FY 2003 Cost	FY 2003 Cost	FY 2003 Award Date	FY 2004 Cost	FY 2004 Award Date	FY 2005 Cost	FY 2005 Award Date	Cost to Complete	Total Cost	Target Value of Contract
(U) Product Development												
Science Applications International Corporation (SAIC) -- Common User Application Software (CUAS) Development	C/GSA BPA	SAIC, San Diego CA	7.320	2.997	May-98	0.000		0.000		Continuing	TBD	TBD
MITRE -- Technical Support of CUAS	S/FFRDC	AF Cryptologic Support Group (CPSG), Lackland AFB TX	3.240	1.246	Nov-00	0.000		0.000		Continuing	TBD	TBD
Windmill International, Inc. -- COMSEC Account Application Software Development	C/GSA BPA	Windmill International, Nashua NH	0.000	0.101	Nov-01	0.000		0.000		Continuing	TBD	TBD
Subtotal Product Development			10.560	4.344		0.000		0.000		Continuing	TBD	TBD
Remarks: All program efforts and funding moved to PE 0303140F, Information Systems Security Program, under the same Project number and Project name effective with the FY04 President's Budget submittal												
(U) Total Cost			10.560	4.344		0.000		0.000		Continuing	TBD	TBD

Exhibit R-4, RDT&E Schedule Profile		DATE February 2004
BUDGET ACTIVITY **07 Operational System Development**	PE NUMBER AND TITLE **0303401F Communications Security**	PROJECT NUMBER AND TITLE **4861 Cryptologic 2000**

Exhibit R-4: BPAC 4861 Cryptologic 2000

Fiscal Year	FY 03				FY 04				FY 05				FY 06				FY 07				FY 08				FY 09			
	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 Key Mgmt. Infrastructure																												
User Application Software Development																												
Transfer Enterprise Data Warehouse Cong add						△																						
Transfer svs support ISSP for Northcom Cng 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 2004

BUDGET ACTIVITY	PE NUMBER AND TITLE	PROJECT NUMBER AND TITLE
07 Operational System Development	**0303401F Communications Security**	**4861 Cryptologic 2000**

(U) Schedule Profile	FY 2003	FY 2004	FY 2005
(U) Continue End User Application Software Development, Common UAS, and KOV-21 integration.	1-4Q		