2016
Major Automated Information System
Annual Report

Key Management Infrastructure Increment 2 (KMI Inc 2)

Defense Acquisition Management
Information Retrieval
(DAMIR)

Table of Contents

Common Acronyms and Abbreviations for MAIS Programs

Acq O&M - Acquisition-Related Operations and Maintenance
ADM - Acquisition Decision Memorandum
AoA - Analysis of Alternatives
ATO - Authority To Operate
APB - Acquisition Program Baseline
BY - Base Year
CAE - Component Acquisition Executive
CDD - Capability Development Document
CPD - Capability Production Document
DAE - Defense Acquisition Executive
DoD - Department of Defense
DoDAF - DoD Architecture Framework
FD - Full Deployment
FDD - Full Deployment Decision
FY - Fiscal Year
IA - Information Assurance
IATO - Interim Authority to Operate
ICD - Initial Capability Document
IEA - Information Enterprise Architecture
IOC - Initial Operational Capability
IP - Internet Protocol
IT - Information Technology
KPP - Key Performance Parameter
$M - Millions of Dollars
MAIS - Major Automated Information System
MAIS OE - MAIS Original Estimate
MAR – MAIS Annual Report
MDA - Milestone Decision Authority
MDD - Materiel Development Decision
MILCON - Military Construction
MS - Milestone
N/A - Not Applicable
O&S - Operating and Support
OSD - Office of the Secretary of Defense
PB - President’s Budget
RDT&E - Research, Development, Test, and Evaluation
SAE - Service Acquisition Executive
TBD - To Be Determined
TY - Then Year
U.S.C- United States Code
USD(AT&L) - Under Secretary of Defense for Acquisition, Technology, & Logistics

Program Information

Program Name

Key Management Infrastructure Increment 2 (KMI Inc 2)

DoD Component

DoD

The acquiring DoD Component is the National Security Agency (NSA).

Responsible Office

Program Manager

Ms. Kimberly Marino
9800 Savage Road
I23K, Suite 6591
Fort Meade, MD 20755-6591

kamarin@nsa.gov

Phone: 240-373-5700
Fax:
DSN Phone:
DSN Fax:
Date Assigned: April 6, 2015

References

MAIS Original Estimate

October 31, 2012

Approved APB

Approved Acquisition Program Baseline (APB) dated January 15, 2013

Program Description

Key Management Infrastructure (KMI) is a unified, scalable, interoperable, and trusted infrastructure that provides net-centric key management services to systems that rely on cryptography, serving Department of Defense (DoD) and the broader cryptographic community. KMI builds on the foundation for a new automated infrastructure to deliver key management products and services to support the Warfighter's Net-Centric Environment.

KMI was designated an Acquisition Category IAM Major Automated Information System program on December 2, 2004. The Assistant Secretary of Defense for Networks and Information Integration (ASD NII) was designated as the Milestone Decision Authority (MDA). The MDA approved a combined Milestone A/B decision on April 16, 2007 and authorized the program to enter the System Development & Demonstration phase for Capability Increment 2 (CI-2). CI-2 was divided into Spiral 1 and Spiral 2. On January 11, 2012, ASD NII was disestablished by order of the Secretary of Defense and the DoD Chief Information Officer was assigned as the KMI MDA. General Dynamics C4 Systems Inc.completed development of Spiral 1 in December 2012. The Spiral 2 development contract was awarded on July 31, 2012 to Science Applications International Corporation. The MDA approved a Milestone C for Spiral 1 Production and Deployment on October 28, 2011, and approved increasing the Low Rate Initial Production Contract quantities to 400 on September 22, 2012. On December 11, 2015, the MDA approved a limited fielding decision for KMI Spiral 2, Spin 1 capabilities to replace legacy system cryptographic accounts worldwide.

To support the Cryptographic Modernization (CM) Mission Area Needs Statement (MNS) objectives and the Global Information Grid (GIG) Information Assurance (IA) strategy, development of the DoD KMI is a critical foundation element for ensuring an adequate security posture for national security systems by providing transparent cryptographic capabilities consistent with operational imperatives and mission environments. As a critical enabler to CM MNS objectives and the GIG IA strategy, the DoD KMI will be realized by the steady rollout of spirals to deliver time-phased capability increments toward end-state IA objectives consistent with the overarching GIG and CM capability requirements. The focus of KMI CI-2 is to build the foundation for the future management of Type 1 and Type 2 key material in a general-purpose networking environment. KMI CI-2 provides Type 1 and 2 key management services and cryptographic products to human users and devices (hereinafter referred to as "supported" or "security-enabled") to enable secure communications. The objectives for KMI CI-2 are: (1) Establish a secure net presence for KMI for Type 1 and Type 2 Key Management; (2) Enable customer transition from the Electronic Key Management System to KMI; (3) Provide web-based key ordering and distribution, enrollment, accounting, compromise recovery, etc. for all key types; and (4) Provide Over-the-Network-Keying to deliver software for KMI-Aware End Cryptographic Units and the KMI Client Node.

Business Case

Business Case Analysis, including the Analysis of Alternatives: Key functional requirements for this program (which were articulated in the KMI Capability Development Document (approved by Joint Requirements Oversight Council Memorandum (JROCM) 247-05 on November 14, 2005) and revalidated in the KMI Capabilities Production Document (CPD) (approved by JROCM 014-12 on February 9, 2012)) are to build the foundation for the future management of key material to support Net-Centric Warfighter operations while also providing enhanced key management capabilities to support legacy strategic and operational Warfighter requirements. Additionally, KMI Capability Increment 2 (CI-2) enables operational commanders to have broader flexibility to coordinate protection of national strategic information, information-based processes, and information system assets within their respective theaters of operation. Guidance for the Analysis of Alternatives (AoA) was issued December 21, 2004. The ensuing AoA considered the legacy Electronic Key Management System (EKMS), a modified EKMS system, a CI-2/CI-3 developmental alternative, and a transformational alternative. The AoA resulted in a recommendation to proceed with the Incremental CI-2/CI-3 alternative. An Economic Analysis (EA) was then performed on the selected alternative. Approval from the Milestone Decision Authority (MDA) was received in an Acquisition Decision Memorandum (ADM), “KMI Milestone B System Development and Demonstration Decision,” April 16, 2007. A Milestone C decision was approved by the MDA on October 28, 2011 via a signed ADM. A revised EA will be developed to support the Full Deployment Decision for the program. CI-2, Spiral 2 introduces new mission capabilities/functionalities, to include Over the Net Keying, key provisioning support for Advanced Extremely High Frequency system, F-22 system and Mobile User Objective System. Spiral 2 was procured using an Agile Software Development methodology with capability delivered yearly with a subset of capability enhancements. By planning for more focused, shorter development and swift delivery of capabilities cycles, the Spiral 2 program is able to greatly reduce the timeframe for deploying critical mission requirements to the warfighter.

Firm, Fixed-Price Feasibility: The determination of the development/integration contract type was based on cost and technical risk associated with satisfying the requirement. The MDA has selected a cost-type contract because development tasks are sufficiently complex and technically challenging that it is impossible to precisely estimate the cost of satisfying the requirements, and it is not practicable to reduce cost and technical risk to a level that would permit the use of a fixed-price contract. KMI is a National Security System that has critical cryptographic and information assurance requirements that must be traded against the system performance requirements during the execution of the development contracts making it difficult to develop relevant measurable performance metrics. Additionally the Spiral 2 contract will be a Cost Plus Award Fee/Incentive Fee contract.

Independent Cost Estimate: In January 2012, the Senior Official determined that the program experienced a Critical Change, and the independent cost estimate completed as part of the program evaluation resulted in the Department of Defense Chief Information Officer restructuring the program by increasing the duration of program development by 12 months resulting in a Full Deployment Decision in April 2017 and by increasing the program costs by $49 million of Research, Development, Test and Evaluation funding across the Future Years Defense Program. Additionally, an ADM included directives to increase stakeholder interaction, create a structured framework of user involvement, and strengthen the use of metrics to develop forecasts and track performance.

A revised cost estimate was conducted by the NSA independent cost team to support the Milestone C decision. The revised cost estimate includes the new threshold and objective requirements outlined in the CPD, which resulted in a critical change for the program. The Director Cost Assessment and Program Evaluation completed an independent cost evaluation of the program during the Critical Change process which was used to inform the updated Acquisition Program Baseline.

Certification of Business Case Alignment; Explanation: I certify that all technical and business requirements have been reviewed and validated to ensure alignment with the business case. This certification is based on my review of the KMI business case including the CPD, AoA, and EA described above.

Business Case Certification:

Name:	Ms. Jennifer S. Walsmith
Organization:	National Security Agency for KMI Inc 2
CAC Subject:	CN=WALSMITH.JENNIFER.S.9000020748,CSS,OU=NSA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US
Date:	4/23/2013 10:44 AM

Business Case Changes

No significant change to the Business Case and Certification.

Significant Change: The program is projecting a 10-month schedule delay for the achievement of the Full Deployment Decision. Per 10 U.S.C. Chapter 144A, the Senior Official will notify Congress of the Significant Change.

Program Status

Significant Change: The program is projecting a 10-month schedule delay for the achievement of the Full Deployment Decision. Per 10 U.S.C. Chapter 144A, the Senior Official will notify Congress of the Significant Change.

Schedule

Schedule Events		
Events	**Original Estimate Objective**	**Current Estimate (Or Actual)**
Full Rate Production (KMI Client HW)[1]	Jun 2013	Jun 2013
KMI CI-2 Full Deployment Decision[2]	Apr 2017	Feb 2018
KMI CI-2 Full Deployment	TBD	TBD

Memo

1/ Full Rate Production (KMI Client HW) provides authorization for fielding of the KMI Client HW with Spiral 1 Software functionality to operational locations in support of operational missions.
2/ KMI CI-2 Full Deployment Decision is based upon the KMI program's readiness to deliver all capabilities in the Capability Production Document.

Acronyms and Abbreviations

CI-2 - Capability Increment 2
HW - Hardware
KMI - Key Management Infrastructure

Performance

Performance Characteristics		
Original Estimate Objective/Threshold		**Current Estimate (Or Actual)**
Deliver Cryptographic Products: Pull (user initiated) Product Delivery		
KMI interfaces shall support pull product delivery. The pull product delivery shall be validated for integrity thus ensuring the product requested is the product received. • 100% of products requested were received with data integrity.	KMI interfaces shall support pull product delivery. The pull product delivery shall be validated for integrity thus ensuring the product requested is the product received. • 100% of products requested were received with data integrity.	Threshold met during Spiral 1 IOT&E and FOT&E.
Connected Networks: Network Identification		
KMI products and services shall be provided to KMI clients via the following networks: Spiral 1: a. SIPRNET (tactical & strategic); b. NIPRNET (tactical & strategic); c. Internet; d. PSTN; and e. JWICS. Spiral 2: a. SIPRNET (tactical & strategic); b. NIPRNET (tactical & strategic); c. Internet; d. PSTN; e. JWICS	KMI products and services shall be provided to KMI clients via the following networks: Spiral 1: SIPRNET (both tactical and strategic). Spiral 2: a. SIPRNET (both tactical and strategic); b. NIPRNET (both tactical and strategic); c. Internet; d. PSTN.	Spiral 1 Threshold met during Spiral 1 IOT&E and FOT&E. Spiral 2 Threshold requirement will be tested during Spiral 2 FOT&E.
Connected Networks: KMI-Aware Device Identification		
KMI products and services shall be provided to KMI-Aware devices via the following networks: Spiral 1: SIPRNET (tactical and strategic) for infrastructure KMI Aware devices. Spiral 2: SIPRNET (tactical and strategic); NIPRNET (tactical and strategic); Public Internet; and JWICS.	KMI products and services shall be provided to KMI-Aware devices via the following networks: Spiral 1: SIPRNET (tactical and strategic) for infrastructure KMI Aware devices. Spiral 2: SIPRNET (tactical and strategic); NIPRNET (tactical and strategic); and Public Internet.	Spiral 1 Threshold met during Spiral 1 IOT&E and FOT&E. Spiral 2 Threshold requirement will be tested during Spiral 2 FOT&E.
CI-2 Net Readiness		
KMI must fully support execution of all critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DoDAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1. Solution architecture products compliant with DoD Enterprise Architecture based on integrated DoDAF content, including specified operationally effective information exchanges; 2. Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in	KMI must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DoDAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1. Solution architecture products compliant with DoD Enterprise Architecture based on integrated DoDAF content, including specified operationally effective information and exchanges; 2. Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules	Threshold met during Spiral 1 IOT&E and FOT&E.

the DoD IEA, excepting tactical and non-IP communications; 3. Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GESPs necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solutions architecture views; 4. Information Assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an ATO by the DAA; and 5. Supportability requirements to include SAASM, Spectrum and JTRS requirements.	identified in the DoD IEA, excepting tactical and non-IP communications; 3. Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GESPs necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solutions architecture views; 4. IA requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an IATO or ATO by the DAA; and 5. Supportability requirements to include SAASM, Spectrum and JTRS requirements.	
Interoperability: Maintain Generated Security Objects		
The KMI shall maintain the following KMI Generated Security Objects: KMI Manager public key certificates, KMI User public key certificates, KMI Device public key certificates, KMI CRLs, and KMI CKLs 1. The KMI shall establish and maintain an archive of the security objects it generates in order to facilitate historical access to information protected by the security-enabled applications it supports. 2. The storage of information in the KMI archive shall meet the requirements of existing Records Management laws, rules, and guidelines. 3. The KMI shall provide guidelines and procedures for access to, and use of the security objects stored in the archive. 4. The KMI archive shall comply with IDM requirements for semantic tagging, search accuracy, and relevance of information returned from a search, as identified in the GIG-IA ICD. 5. IDM semantic tagging and search accuracy and relevance requirements shall be applied to that portion of the KMI archive that is accessible online for search and retrieval of information, as appropriate.	The KMI shall maintain the following KMI Generated Security Objects: KMI Manager public key certificates, KMI User public key certificates, KMI Device public key certificates, KMI CRLs, and KMI CKLs 1. The KMI shall establish and maintain an archive of the security objects it generates in order to facilitate historical access to information protected by the security-enabled applications it supports. 2. The storage of information in the KMI archive shall meet the requirements of existing Records Management laws, rules, and guidelines. 3. The KMI shall provide guidelines and procedures for access to, and use of the security objects stored in the archive.	Threshold met during Spiral 1 IOT&E and FOT&E.
CI-2 Logistics and Readiness: Operational Availability		
The overall KMI system shall have an Ao of 0.9999 (not including external communications interruptions).	The overall KMI system shall have an Ao of 0.9980 (not including external communications interruptions).	Threshold met during Spiral 1 IOT&E.
Survivability		
KMI Client Node shall protect key products and other sensitive data stored at the client from unauthorized access impacting the survivability of other warfighter systems.	KMI Client Node shall protect key products and other sensitive data stored at the client from unauthorized access impacting the survivability of other warfighter systems.	Threshold met during Spiral 1 IOT&E and FOT&E.

Memo

The KMI Key Performance Parameters are defined in the August 12, 2011 KMI Capabilities Production Document.

Acronyms and Abbreviations

Ao - Operational Availability
CI-2 - Capability Increment Two
CKLs - Compromised Key Lists
CRLs - Certificate Revocation Lists
DAA - Designated Accrediting Authority
FOT&E - Follow-On Test & Evaluation
GESPs - GIG Enterprise Service Profiles
GIG - Global Information Grid
IDM - Information Dissemination Management
IOT&E - Initial Operational Test & Evaluation
JTRS - Joint Tactical Radio System
JWICS - Joint Worldwide Intelligence Communications System
KMI - Key Management Infrastructure
NIPRNET - Non-Secure INternet Protocol Router Network
PSTN - Public Switch Telephone Network
SAASM - Selective Availability Anti-Spoofing Module
SIPRNET - Secret Internet Protocol Router Network
TV-1 - Technology View 1

Cost

KMI Inc 2				
Appropriation Category	BY 2005 $M		TY $M	
	Original Estimate	Current Estimate Or Actual	Original Estimate	Current Estimate Or Actual
Acquisition Cost				
RDT&E	459.2	467.1	529.3	539.3
Procurement	0.0	0.0	0.0	0.0
MILCON	0.0	0.0	0.0	0.0
Acq O&M	0.0	0.0	0.0	0.0
Total Acquisition Cost	459.2	467.1	529.3	539.3
Operating and Support (O&S) Cost				
Total Operating and Support (O&S) Cost	115.6	118.7	149.9	163.4
Total Life-Cycle Cost				
Total Life-Cycle Cost	574.8	585.8	679.2	702.7

Cost Notes

1. This report and the Budget Year IT-1 Exhibit cover different time periods thus the costs will not match.
2. Then Year dollars are included for information purposes only; cost variances will be reported against Base Year dollars.
3. The O&S costs reflect all work performed during that phase, regardless of the type or source of funding.