PART I - A

PART I: SUMMARY INFORMATION AND JUSTIFICATION
In Part I, complete Sections A. B, C, and D for all capital assets (IT and non-IT). Complete Sections E and F for IT capital assets.
OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section A: Overview (All Capital Assets)
I.A.1) Date of Submission (mm/dd/yyyy)
Dec 12, 2008
I.A.2) Agency
029 - Department of Veterans Affairs
I.A.3) Bureau
00 - Agency Wide Initiatives
I.A.4) Name of this Investment:(SHORT ANSWER)
Enterprise Cyber Security Program -2010
I.A.5) Unique Project(Investment) Identifier: Update the UPI using the Exhibit 53 tab.
029-00-01-25-01-5104-00
I.A.6) What kind of investment will this be in FY2010? (Please NOTE: Investments moving to O&M in FY2010, with Planning/Acquisition activities prior to FY2010 should not select O&M. These investments should indicate their current status.)
Operations and Maintenance
I.A.7) What was the first budget year this investment was submitted to OMB?
FY2004
I.A.8) Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap: (LONG ANSWER)
This investment funds the programs that provide VA with IT security policy, guidance, tools, advice and general support. Included are related field operations and staffing, incident response and risk management, oversight and compliance review and continuity of operations planning (COOP). Staff develops, distributes and maintains IT security policy, guidance and standards based on Federal law and requirements. Security Reporting and Management oversees the Certification and Accreditation (C&A) and Federal Information Security Management Act (FISMA) compliance and reporting programs, and the assessment and testing of the security controls. Also provided are procurement, accounting, budget and HR support for the investment. Critical Infrastructure Protection operates the network and system operation center (NSOC) for incident reporting and response as well as other VA security services such as penetration testing, vulnerability scanning, firewall management, intrusion detection monitoring. Information Protection and Risk Management promotes data identity protection awareness, through the Enterprise Identity Safety effort, and has ready services such as digital forensics and credit monitoring to evaluate the risk and response following a security breach. COOP identifies essential IT functions and maintains the alternate operations site for use in the event of a disaster. Enterprise Security Service reviews tools, products and equipment prior to purchase to ensure that they meet security requirements. It sends security related software patches and updates to the field and supports the VA capability to protect data during transmission and storage through the use of encryption tools and access right controls. Field Security Service (FSS) directs the Information Security Officers (ISO) throughout VA. The ISOs work with the IT system managers to complete the on-going C&A work and FISMA reporting for over 580 VA IT systems. FSS, in collaboration with Security Reporting and Management staff, monitors the assessment work and the plan of action to remedy any identified problems. The recently formed Oversight and Compliance program has the special mission of conducting site assessments to measure compliance to IT security and privacy policies and standards. This investment also coordinates VA security awareness training, role-based training for ISOs, and the VA's annual IT Security Conference. The E-authentication effort is also funded by this investment.
I.A.9) Did the Agency's Executive/Investment Committee approve this request?
Yes
I.A.9.a) If "yes," what was the date of this approval?
Dec 10, 2008

I.A.10) Did the Project Manager review this Exhibit?

Yes

I.A.11) Contact information of Program/Project Manager?

	Project Managers Names (SHORT ANSWER)	PM Phone	E-mail (SHORT ANSWER)
Primary in-house	Ruth Anderson	202-273-9842	ruth.anderson@va.gov

I.A.11.a) What is the current FAC-P/PM (for civilian agencies) or DAWIA (for defense agencies) certification level of the program/project manager?

I.A.11.b) When was the Program/Project Manager Assigned?

Aug 1, 2007

I.A.11.c) What date did the Program/Project Manager receive the FACP/PM certification? If the certification has not been issued, what is the anticipated date for certification?

Mar 21, 2007

I.A.12) Has the agency developed and/or promoted cost effective, energy-efficient and environmentally sustainable techniques or practices for this project.

No

I.A.12.a) Will this investment include electronic assets (including computers)?

No

I.A.12.b) Is this investment for construction or retrofit of a federal building or facility? (Answer applicable to non-IT assets only)

No

I.A.12.b.1) If "yes," is an ESPC or UESC being used to help fund this investment?

I.A.12.b.2) If "yes," will this investment meet sustainable design principles?

I.A.12.b.3) If "yes," is it designed to be 30% more energy efficient than relevant code? (Answer applicable to non-IT assets only)

I.A.13) Does this investment directly support one of the PMA initiatives?

Yes

I.A.13.a) If "yes," check all that apply:

	PMA Initiatives for XML Submission	PMA Initiatives
		- Human Capital
		- Budget Performance Integration
		- Financial Performance
Yes	Expanded E-Government	- Expanded E-Government
		- Competitive Sourcing
		- Faith Based and Community
		- Real Property Asset Management
		- Eliminating Improper Payments
		- Privatization of Military Housing

		- Research & Development Investment Criteria
		- Housing & Urban Development Management & Performance
		- Broadening Health Insurance Coverage through State Initiatives
		- "Right Sized" Overseas Presence
		- Coordination of VA & DoD Programs and Systems

I.A.13.b) Briefly and specifically describe for each selected how this asset directly supports the identified initiative(s)? (e.g. If E-Gov is selected, is it an approved shared service provider or the managing partner?)(MEDIUM ANSWER)

The investment addresses the goal of Expanded E-Governance. In cooperation with the development group, this investment funds the design, deployment and maintenance of the E-authentication infrastructure. E-authentication allows veterans as outside users to securely access specific IT systems via web interfaces in order to make use of services provided by VA. This investment pays for the maintenance of VA's PKI certificates and provides PKI help desk support.

I.A.14) Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.)

No

I.A.14.a) If "yes," does this investment address a weakness found during a PART review?

I.A.14.b) If "yes," what is the name of the PARTed program? (SHORT ANSWER)

I.A.14.c) If "yes," what rating did the PART receive?

I.A.15) Is this investment information technology? (See section 53.8 for definition)

Yes

I.A.16) What is the level of the IT Project? (per CIO Council PM Guidance)

Level 1

I.A.17) What project management qualifications does the Project Manager have? (per CIO Council PM Guidance)

Qualification Status	Qualification Status for XML Submission	Description
1	(1) Project manager has been validated as qualified for this investment	(1) - Project manager has been validated as qualified for this investment.
		(2) - Project manager qualification is under review for this investment.
		(3) - Project manager assigned to investment, but does not meet requirements.
		(4) - Project manager assigned but qualification status review has not yet started.
		(5) - No Project manager has yet been assigned to this investment.

I.A.18) Is this investment or any project(s) within this investment identified as "high risk" on the Q4-FY 2008 agency high risk report (per OMB Memorandum M-05-23)

No

I.A.19) Is this project (investment) a Financial Management System? (see section 53.3 for definition)

No

I.A.19.a) If so, does this project (investment) address a FFMIA (Federal Financial Managers Integrity Act) compliance area?

I.A.19.a.1) If yes, which compliance area?

I.A.19.a.2) If "no," what does it address? (MEDIUM ANSWER)

This investment, the Information Protection and Risk Management Program (IPRM)/Cyber Security is not a system but is a collection of programs that provides IT security guidance, policy, tools and other support to all VA employees who make use of computers or automated systems.

I.A.19.b) If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A–11 section 52 (LONG ANSWER)

Not applicable

I.A.20) What is the percentage breakout for the total FY2010 funding request for the following? (This should total 100%)

Percentage of Total Investment	
% Hardware	
% Software	
% Services	
% Others	

I.A.21) If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities?

NA

I.A.22) Contact information of individual responsible for privacy related questions:

Contact Name: (SHORT ANSWER)	Ray Poore
Phone Number:	(202) 461-7450
Title: (SHORT ANSWER)	Deputy Associate Deputy Assistant Secretary for Privacy and Risk Management
E-mail: (SHORT ANSWER)	ray.poore@va.gov

I.A.23) Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?

Yes

I.A.24) Does this investment directly support one of the GAO High Risk Areas?

Yes

PART I - B

PART I: SUMMARY INFORMATION AND JUSTIFICATION

In Part I, complete Sections A. B, C, and D for all capital assets (IT and non-IT). Complete Sections E and F for IT capital assets.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section B: Summary of Funding (All Capital Assets)

I.B.1) FILL IN TABLE IN CURRENT VALUES (in millions)

(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)

Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are

rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be EXCLUDED from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The total estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

Category of Funds	PY-1 and Earlier	PY 2008	CY 2009	BY 2010
Planning Total	0.000	0.000	0.000	0.000
Acquisition Total	0.000	0.000	0.000	0.000
Operations & Maintenance Total	225.734	56.384	75.035	85.038
Total, All Stages (Non-FTE)	225.734	56.384	75.035	85.038
Government FTE Costs	69.325	65.688	65.473	78.364
Govt. FTE Numbers	451	467	587	616
Total (FTE and Non-FTE)	295.059	122.072	140.508	163.402

Government FTE Costs SHOULD NOT be INCLUDED as part of the TOTAL, All Stages Resources represented.

Note: 1) For the cross-agency investments, this table should include all funding (both managing partner and partner agencies). 2) Total, All Stages Resources should equal Total, All Stages Outlays.

I.B.2) Will this project require the agency to hire additional FTE's?

Yes

I.B.2.a) If Yes, How many and in what year? (MEDIUM ANSWER)

579 FTE on board as of November 2008. The program is continuing to hire for the ISO interns and for CIP and Cyber Security groups. Field Services, which is the Information Security Officer's program, is expanding its coverage of facilities and clinics and is hiring ISO interns to continue the steps of training and skill building necessary for them to assume full ISO responsibilities. 309 ISOs and 120 interns.

I.B.3) If the summary of spending has changed from the FY2009 President's budget request, briefly explain those changes. (LONG ANSWER)

PART I - C

PART I: SUMMARY INFORMATION AND JUSTIFICATION

In Part I, complete Sections A. B, C, and D for all capital assets (IT and non-IT). Complete Sections E and F for IT capital assets.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section C: Acquisition/Contract Strategy (All Capital Assets)

I.C.1) If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why? (LONG ANSWER)

This investment is in a steady state operational phase. The contracts under this investment do not address software development or have similar elements that would cause earned value criteria to be part of the contract language. These contracts make use of simplified contracting vehicles. Managers are able to track purchases, costs, delivery and installations, as necessary.

I.C.2) Do the contracts ensure Section 508 compliance?
Yes
I.C.2.a) Explain why not or how this is being done? (MEDIUM ANSWER)
The GSA Federal Supply Schedule contracts, under which the BPA orders are issued, specify Section 508 compliance. The mechanism for validating compliance includes routine reviews and assessments of associated products and websites, as well as automated scanning tools.
I.C.3) Is there an acquisition plan which has been approved in accordance with agency requirements?
Yes
I.C.3.a) If "yes," what is the date?
May 24, 2007
I.C.3.a.1) Is it Current?
Yes
I.C.3.b) If "no," will an acquisition plan be developed?
I.C.3.b.1) If "no," briefly explain why: (MEDIUM ANSWER)

PART I - D

PART I: SUMMARY INFORMATION AND JUSTIFICATION

In Part I, complete Sections A. B, C, and D for all capital assets (IT and non-IT). Complete Sections E and F for IT capital assets.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section D: Performance Information (All Capital Assets)

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures (indicators) must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency (e.g.,improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative measure.

Agencies must use the following table to report performance goals and measures for the major investment and use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM. There should be at least one Measurement Indicator for each of the four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov. The table can be extended to include performance measures for years beyond the next President's Budget.

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Grouping	Measurement Indicator	Baseline	Planned Improvements to the Baseline	Actual Results
2008	Public Health & Socioeconomic Wellbeing	Processes and Activities	Cycle Time	Complete C&A activities for all operational systems, on a 3-three recurring cycle	Certify the security controls tested so that 95% of the It systems will continue with their authority to operate.	No percentage improvement. The goal is to continue this operational performance.	The security controls tested allowed 95% or more of the systems to continue their authority to operate

2008	Public Health & Socioeconomic Wellbeing	Technology	IT Contribution to Process, Customer, or Mission	Implement Health Risk reporting at the facility level within SMART.	During FY 2008 the health risk reporting was not yet established. It will be completed in FY 2009	The goal is to begin the implementation of the health risk reporting during FY 2009	Work to implement the health risk reporting at the facility level will begin in FY 2009
2008	Public Health & Socioeconomic Wellbeing	Mission and Business Results	Health Care Administration	Annual IT security awareness training	95% of all employees will complete the annual training. The remaining 5% will not due to extended sick leave or call to military service	No percentage improvement. Goal is to continue this operational performance.	The percentage of employees completing the annual IT security awareness training met the goal. The exact figure is being checked.
2008	Public Health & Socioeconomic Wellbeing	Customer Results	Customer Training	To measure tangible impact to the customer as a result of role-based IT security training, to receive credit for the training the individual must pass a mandatory test by correctly answering at least 80% of the test questions.	The baseline would be to have 95% of those completing the training pass the mandatory test and receive their credit hours.	The goal is to maintain this level of operational performance.	All those completing the training passed the test
2009	Public Health & Socioeconomic Wellbeing	Processes and Activities	Cycle Time	Complete C&A activities for all operational systems, on a 3-three recurring cycle	Certify the security controls tested so that 95% of the It systems will continue with their authority to operate.	No percentage improvement. The goal is to continue this operational performance.	
2009	Public Health & Socioeconomic Wellbeing	Technology	IT Contribution to Process, Customer, or Mission	Implement Health Risk reporting at the facility level within SMART.	This will provide management with a security health risk assessment of all systems by facility with recommended steps to improve security controls, documentation, and POA&M remediation.	Provide scorecards by system for POAMs and C&A goals.	

2009	Public Health & Socioeconomic Wellbeing	Mission and Business Results	Health Care Administration	Annual IT security awareness training	95% of all employees will complete the annual training. The remaining 5% will not due to extended sick leave or call to military service	No percentage improvement. Goal is to continue this operational performance.	
2009	Public Health & Socioeconomic Wellbeing	Customer Results	Customer Training	To measure tangible impact to the customer as a result of role-based IT security training, to receive credit for the training the individual must pass a mandatory test by correctly answering at least 80% of the test questions.	The baseline would be to have 95% of those completing the training pass the mandatory test and receive their credit hours.	The goal is to maintain this level of operational performance.	
2010	Public Health & Socioeconomic Wellbeing	Processes and Activities	Cycle Time	Complete C&A activities for all operational systems, on a 3-three recurring cycle	Certify the security controls tested so that 95% of the It systems will continue with their authority to operate.	No percentage improvement. The goal is to continue this operational performance.	
2010	Public Health & Socioeconomic Wellbeing	Technology	IT Contribution to Process, Customer, or Mission	Implement Health Risk reporting at the facility level within SMART.	This will provide management with a security health risk assessment of all systems by facility with recommended steps to improve security controls, documentation, and POA&M remediation.	Broaden metrics to include Privacy and general documentation	
2010	Public Health & Socioeconomic Wellbeing	Mission and Business Results	Health Care Administration	Annual IT security awareness training	95% of all employees will complete the annual training. The remaining 5% will not due to extended sick leave or call to military service	No percentage improvement. Goal is to continue this operational performance.	

2010	Public Health & Socioeconomic Wellbeing	Customer Results	Customer Training	To measure tangible impact to the customer as a result of role-based IT security training, to receive credit for the training the individual must pass a mandatory test by correctly answering at least 80% of the test questions.	The baseline would be to have 95% of those completing the training pass the mandatory test and receive their credit hours.	The goal is to maintain this level of operational performance.	

PART I - F

PART I: SUMMARY INFORMATION AND JUSTIFICATION

In Part I, complete Sections A. B, C, and D for all capital assets (IT and non-IT). Complete Sections E and F for IT capital assets.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section F: Enterprise Architecture (EA) (IT Capital Assets only)

In order to successfully address this area of the business case and capital asset plan you must ensure the investment is included in the agency's EA and Capital Planning and Investment Control (CPIC) process, and is mapped to and supports the FEA. You must also ensure the business case demonstrates the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

I.F.1) Is this investment included in your agency's target enterprise architecture?

Yes

I.F.1.a) If "no," please explain why? (LONG ANSWER)

I.F.2) Is this investment included in the agency's EA Transition Strategy?

Yes

I.F.2.a) If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment. (MEDIUM ANSWER)

VA Enterprise Cyber Security Program

I.F.2.b) If "no," please explain why? (LONG ANSWER)

I.F.3) Is this investment identified in a completed (contains a target architecture) and approved segment architecture?

Yes

I.F.3a) If "yes," provide the six digit code corresponding to the agency segment architecture. The segment architecture codes are maintained by the agency Chief Architect.

700-000

Segment Architecture Mapping Reference Table:

BUSINESS SEGMENT NAME	SEGMENT ARCHITECTURE CODE
1) Health Business Segment	**100-000**
2) Benefits Business Segment	**200-000**
3) Memorial, Burials & HQ Segment	**300-000**
4) Material Management Segment	**400-000**
5) Financial Segment	**500-000**
6) Human Resources Segment	**600-000**
7) Security Management Segment	**700-000**
8) Information Management Segment	**800-000**
9) Education & Training Segment	**900-000**

I.F.3) FEA SERVICE REFERENCE MODEL:

I.F.3) Identify the service components funded by this major IT investment (e.g.,knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.whitehouse.gov/omb/egov/.

SERVICE COMPONENT TABLE:

	Agency Component Name(SHORT ANSWER)	Agency Component Description (MEDIUM ANSWER)	FEA SRM Service Type	FEA SRM Component (a*)	FEA Service Component Reused : Component Name (b*)	FEA Service Component Reused : UPI (b*)	Internal or External Reuse? (c*)	BY Funding Percentage (d*)
1	E-Authentication	Establishes the mechanism to allow Veterans to electronically identify and authenticate themselves to any e-gov/e-auth - compliant web-based service offered by VA and other Federal government agencies using the same credential.	Security Management	Identification and Authentication			No Reuse	

2	Cyber Security Section	Management of Cyber Security policy development, verification of security controls, FISMA reporting and audit response' and C&A.	Security Management	FISMA Management and Reporting			No Reuse	
3	Critical Infrastructure protection	Provides many network based security products including virus protection, PKI certificates, intrusion prevention and router access control	Security Management	Virus Protection			No Reuse	
4	Information Security Field Operations	Provides management support for district ISOs geographically dispersed throughout US; oversees training, awareness, education, and Professionalism programs.	Security Management	Intrusion Prevention			No Reuse	
5	SIEM - Security Information and Event Management	Is the Agency's Network Security and Operations Center	Security Management	Intrusion Detection			No Reuse	
6	Information Protection and Risk Management	Promotes the awareness of information protection controls and processes	Security Management	Intrusion Prevention			No Reuse	
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								

19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								
39								
40								
41								
42								
43								
44								
45								
46								
47								
48								
49								
50								

NOTE:

(a) - Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.*

(b) - A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.*

(c) - 'Internal' reuse is within an agency. For example, one agency within a department is reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.*

(d) - Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the funding level transferred to another agency to pay for the service.*

I.F.4) FEA TECHNICAL REFERENCE MODEL:

I.F.4) To demonstrate how this major IT investment aligns with Reference Model (TRM), please list the Service Areas, Service Specifications supporting this IT investment.

TECHNICAL REFERENCE MODEL TABLE:

	FEA SRM Component (a*)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard
1	Identification and Authentication	Component Framework	Security	Certificates / Digital Signatures
2	FISMA Management and Reporting	Component Framework	Data Management	Reporting and Analysis
3	Virus Protection	Component Framework	Security	Supporting Security Services
4	Skills Management	Component Framework	Security	Supporting Security Services
5	Issue Tracking	Component Framework	Security	Supporting Security Services
6	Risk Management	Component Framework	Security	Supporting Security Services
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				

24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				

NOTE:

(a) - Service Components identified in the previous question(I.F.3) should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications*

(b) - In the Service Specification field, Agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.*

I.F.5) Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)?

No

I.F.5.a) If "yes," please describe. (LONG ANSWER)

PART III - A

Part III: For "Operation and Maintenance" investments ONLY (Steady State)

Part III should be completed only for investments identified as "Operation and Maintenance" (Steady State) in response to Question 6 in Part I, Section A above.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

Section A - RISK MANAGEMENT (All Capital Assets)

In order to successfully address this issue on the business case and capital asset plan, you must have performed a risk assessment at the initial concept, included mandatory risk elements defined below and demonstrate active management of the risk throughout the life-cycle of the investment.

For all investments, both IT and non-IT, you must discuss each of the following risks and present your plans to eliminate, mitigate, or manage risk, with milestones and completion dates. If there is no risk to the investment achieving its goals from a risk category, indicate so. If there are other risks identified, include them. Risk assessments should include risk information from all stakeholders and should be performed at the initial concept stage and then monitored and controlled throughout the life-cycle of the investment. Risk assessments for all investments must include: 1) schedule ; 2) initial costs; 3) life-cycle costs); 4) technical obsolescence; 5) feasibility; 6) reliability of systems; 7) dependencies and interoperability between this investment and others; 8) surety (asset protection) considerations; 9) risk of creating a monopoly for future procurements; 10) capability of agency to manage the investment; and 11) overall risk of investment failure.

In addition, for IT investments, risk must be discussed in the following categories 12) organizational and change management; 13) business; 14) data/info; 15) technology; 16) strategic; 17) security; 18) privacy; and 19) project resources. For security risks, identify under the Description column the level of risk as high, medium, or basic. What aspect of security determines the level of risk, i.e., the need for confidentiality of information, availability of information or the system, reliability of the information or system? Under the Current Status column, list the milestones remaining to mitigate the risk.

Moreover, for each risk category with a probability of occurrence of at least medium and impact of at least medium, please indicate whether or not the costs to mitigate the risk have been incorporated into your lifecycle cost estimates in the summary of spending stages section of this Exhibit 300. If not, please also indicate why in your response.

III.A.1) Does the investment have a Risk Management Plan?

Yes

III.A.1.a) If "yes," what is the date of the plan?

Dec 1, 2008

III.A.1.b) Has the Risk Management Plan been significantly changed since last year's submission to OMB?

No

III.A.1.c) If "yes," describe any significant changes: (LONG ANSWER)

III.A.2) If there currently is no plan, will a plan be developed?

III.A.2.a) If "yes," what is the planned completion date?

III.A.2.b) If "no," what is the strategy for managing the risks? (LONG ANSWER)

PART III - B

Part III: For "Operation and Maintenance" investments ONLY (Steady State)

Part III should be completed only for investments identified as "Operation and Maintenance" (Steady State) in response to Question 6 in Part I, Section A above.

OMB Text Limitations - SHORT ANSWER(250 Characters), MEDIUM ANSWER(500 Characters) and LONG ANSWER(2500 Characters)

III.B) Cost and Schedule Performance:

III.B.1) Was operational analysis conducted?

No

III.B.1.a) If "yes," provide the date the analysis was completed.

III.B.2) Complete the following table to compare actual performance against the current performance baseline and to the initial performance baseline. In the Current Baseline section, for all milestones listed, you should provide both the baseline and actual completion dates (e.g., "03/23/2003")/ "04/28/2004").

Description of Milestone	Current BL Completion Date Planned	Current BL Completion Date Actual
Public Key Infrastructure & E-Authentication	Sep 30, 2005	Sep 30, 2005
Business Assurance	Sep 30, 2005	Sep 30, 2005
Critical Information Protection	Sep 30, 2005	Sep 30, 2005
Information Security / Field Operations	Sep 30, 2005	Sep 30, 2005
Security Configuration and Management	Sep 30, 2005	Sep 30, 2005
Technology and Integration	Sep 30, 2005	Sep 30, 2005
Public Key Infrastructure & E-Authentication¬	Sep 30, 2006	Sep 30, 2006
Business Assurance	Sep 30, 2006	Sep 30, 2006
Critical Information Protection	Sep 30, 2006	Sep 30, 2006
Information Security / Field Operations	Sep 30, 2006	Sep 30, 2006
Security Configuration and Management	Sep 30, 2006	Sep 30, 2006
Technology and Integration	Sep 30, 2006	Sep 30, 2006
Public Key Infrastructure & E-Authentication¬	Sep 30, 2007	Sep 30, 2007
Business Assurance	Sep 30, 2007	Sep 30, 2007
Critical Information Protection	Sep 30, 2007	Sep 30, 2007
Information Security / Field Operations	Sep 30, 2007	Sep 30, 2007
Security Configuration and Management	Sep 30, 2007	Sep 30, 2007
Technology and Integration	Sep 30, 2007	Sep 30, 2007
Public Key Infrastructure & E-Authentication¬	Sep 30, 2008	Sep 30, 2008
Business Assurance	Sep 30, 2008	Sep 30, 2008
Critical Information Protection	Sep 30, 2008	Sep 30, 2008
Information Security / Field Operations	Sep 30, 2008	Sep 30, 2008
Security Configuration and Management	Sep 30, 2008	Sep 30, 2008
Technology and Integration	Sep 30, 2008	Sep 30, 2008
All 6 program elements	Sep 30, 2009	
All 6 program elements	Sep 30, 2010	
